Master's Thesis

Global Data Governance: The Global Fragmented Data Regulatory Framework and Digital Technology's Role in International Relations Theory

Anna Junker Sohrbeck

Joint Master's Degree in China and International Relations
Aalborg University and University of International Relations (国际关系学院)

Supervisors:
Shi Yadong, *University of International Relations*
Jesper Willaing Zeuthen, *Aalborg University*

Student number:
20211513

Keystrokes: 141.359
Pages: 58.8

May 2023

Abstract

This thesis examines the issue of a global fragmented data regulatory framework when concerning data governance. Because of a lack of international collaboration on creating a framework for data governance, states adopt various approaches, which has a negative effect on the development of global digital infrastructure. To examine the issue of a fragmented data regulatory framework, the thesis conducts a case study analysis of the different data regulatory frameworks implemented by the U.S., the EU, and China. The three have been chosen as cases because of their positions as powerful primary actors in the global political and economic structure, as well as their different approaches to designing data regulatory frameworks. Through the case study analysis, it is determined that all three actors utilise a discursive practice of claiming national security to be an issue of data control, albeit in different ways. This includes securitisation of foreign companies and the use of the notions 'digital sovereignty' and 'cyber sovereignty.' These practices lead to protectionist policies, as the actors want to enhance domestic industries. In wanting to capture the complexity of global data governance and how to analyse it, the thesis forms an extensive theoretical foundation upon which the case study is analysed, based on theories concerning surveillance, territorialisation, and nationalist versus globalist sentiments. It is then questioned how IR theory tends to treat technology in its understanding of international political change, from which this thesis has included realism and constructivism specifically, to better assess technology's relevance in IR theory. The thesis argues that the realist and constructivist frameworks are limited in their understandings of technology, when analysing global data governance, as it is argued that data and digital technology is complex and dynamic in a way that realism and constructivism does not capture. The thesis further concludes that through value-oriented legitimisation, the actors involved are actively trying to influence global data governance.

Table of Contents

INTRODUCTION 5

Introducing the problem 5

METHODOLOGY 7

Qualitative inductive research approach with deductive elements 7
Collection of empirical data and units of analysis: The U.S, the EU, China 8
Case study analysis with document analysis 9
Theoretical considerations 10
Methodological limitations 11

THEORETICAL OVERVIEW 12

Theoretical approaches to technology in international relations 13
Realism 13
Constructivism 16
Deterritorialisation 18
Surveillance capitalism 19
Techno-nationalism, techno-globalism, and neo-techno-nationalism 20

CASE STUDY ANALYSIS 24

THE U.S. 25

U.S. National Security Strategies and data 26
U.S. influence on global data governance 28

THE EU 30

The GDPR framework 31
Digital Sovereignty for Europe 34

THE U.S.-EU PARTNERSHIP AND DATA GOVERNANCE 36

CHINA 37

China's national data regulatory framework 38
China's influence on global data governance 42

SUMMARY 44

THEORETICAL ASSESSMENT 45

FORMING A THEORETICAL FOUNDATION FOR THE SHIFT IN DATA GOVERNANCE 45
GOVERNING DATA ON THE LOCAL AND GLOBAL LEVEL 48
REALIST AND CONSTRUCTIVIST PERSPECTIVES ON THE FRAGMENTED DATA REGULATORY FRAMEWORK.....50

CONCLUSION.....54

BIBLIOGRAPHY.....56

Introduction

Data in its digital form and various shapes has become essential for our digital infrastructure and its further development, which we all depend on in our daily lives, from an individual level to private sector level to institutional level, from domestic to global connections. Hence, data – even in its most undefined conceptualisation, whether it be Big Data, Internet of Things etc. – functions as both a strategic asset, system of information and storage, and necessary evil for all the various connections we depend upon across private, corporate, and institutional structures. Data, either collected digitally or handled digitally, has thus become a new form of currency, which beforehand with unlimited free flow of data were able to be accumulated value from but also misused and exploited.

The importance of data and the structure in which it has evolved within the last few decades has experienced a rapid international digital technological development. This development has taken place across borders and in a pace in which other international standards have not been able to follow regarding setting up structures similar to other existing structures and frameworks designed to safeguard trade, rights, and security. This is especially because most of the digital development upon which we now depend has mainly been driven by the private sector consisting of private corporations having been a part of designing and dominating our global digital framework. In general, it can be argued that digital technology has developed at such a rapid speed that global legal, regulatory, and policy frameworks have not been able to keep up with – the latest example of this being the ongoing debate on artificial intelligence (AI) development and the ethics surrounding it.

Introducing the problem

An aspect of the complicated process of globalisation and an increased localisation of technologies is the question of the free flow of data across borders. Free flow of data has been made possible by globalisation but there is also an increased wish for control of data transfer, which would curb the free flow of data. Simultaneously, technological innovation and competition have become geopolitical hot points for conflict between great powers, and the free flow of data and data protection are included within this geopolitical context. Something that is mostly being done and utilised by private companies and now increasingly being regulated on either national or regional levels. Data is of high importance to the current global structure on many levels, primarily because of the basic acknowledgement that our current flow of information could not exist without data. Data and its flow has thus become of primary

importance to all levels of society – from individuals to civil society, academia, governments, organisations, and the private sector. Data is important to regulate in a proper manner as "a well-designed data governance framework allows countries to capture the full economic and social value of both public intent and private intent data and leverages synergies between them."[1] While data governance frameworks are primarily domestically focused, the World Bank report further explained that the issues and challenges faced are necessary to confront through international collaboration.[2] This is especially important as digital infrastructure is uneven globally, and adequate digital infrastructure is necessary for countries to be able to fully participate in the global data-driven economy.[3] Thus, international collaboration on establishing how to govern data is necessary to further digital development. However, as data has not been regulated evenly globally and countries instead base their data regulations on ground of national needs, it is highly complex to develop a framework of even global data governance.

This thesis chooses to focus on the problem of a globalised technological landscape around the conceptualisation of a 'fragmented data regulatory framework,' which is based on the formulation of "the emergence of a global data governance framework that is transnational in nature and increasingly fragmented by design" by Douglas Arner et al.[4] This conceptualisation covers the lack of an international legal framework to govern the movement, collection, and utilisation of data, which results in different national and regional approaches instead. This fragmentation has created further challenges for global data governance, with a lack of proper protection of personal privacy, questions of security, and challenges to the free flow of data, as these are somewhat conflicting interests. This is because of the general issue of aligning good data protection, free flow of cross-border data, and data protection autonomy simultaneously. In assessing this issue, the three relevant actors identified in this research to examine, the U.S., the EU, and China, are approaching data regulations in widely different ways. All three are major actors within the international political and economic structure, so their approaches to data regulatory frameworks are foundational to the formation of global data governance. However, assessing the subject of a fragmented data regulatory framework raises a question of how to treat technology's influence on international politics. Because in which context do we

[1] World Bank (2021) *World Development Report 2021: Data for Better Lives*. Washington DC: World Bank. P. 10.
[2] Ibid.
[3] World Bank 2021, 12.
[4] Arner, Douglas et al (2022) "The Transnational Data Governance Problem." *Berkeley Technology Law Journal* vol. 37: 625-700. P. 628.

understand global data governance and power? Can we examine and understand different data regulatory frameworks as having an influence on the global distribution of power, or vice versa. Should the fragmented data regulatory framework be understood as a current phenomenon that has resulted from the global distribution of power and great power rivalry? It is from this outset that digital technology's role in international relations matter, because how the subject is conceptually and theoretically approached determines how we further examine its corelation with policy formation, international relations, and global power rivalry. Hence, the research question of this thesis is as follows:

What implications does a global fragmented data regulatory framework hold for global data governance and how can the issue be assessed theoretically?

The units of analysis for this thesis are the U.S., the EU, and China as key actors within the formation of global data governance. The analysis will function as a case study focused on the three key actors' relevant regulatory frameworks, analysing how they might differ or align with one another, as well as the impact it might have on global data governance. How their different approaches might affect global data governance will be analysed through the selected theoretical perspectives and frameworks. This part of the analysis will further examine how data as an essential digital technology hold importance to the structure of international politics, by assessing the relationship between data as important technology and international political change.

Methodology

Qualitative inductive research approach with deductive elements

In approaching the issue of a fragmented data regulatory framework and the questions surrounding how to properly approach the subject as presented in the introduction, this thesis will take an inductive research approach with some deductive considerations. This will be done through the process of not having a clear theoretical approach to the subject of a fragmented data regulatory framework at the offset of the case study analysis. Rather, an extensive selection of theories has been included. Following the case studies, a theoretical assessment will be conducted based on the case study analysis of how three of the key actors are

influencing global data governance within the fragmented data regulatory framework. However, while a wide selection of theories has been included to analytically evaluate the three actors' influence on global data governance, it becomes a mixed approach, based on considerations of their approaches to power, norms, technology, and territoriality, and assessing the relationship between technology and international political change.

Collection of empirical data and units of analysis: The U.S, the EU, China

The empirical data collected to fulfil the case study analysis constitutes of a wide variety of official documents from the three main actors – the U.S., the EU, and China. Considering the difference in political systems ranging from these three actors, as well as the different levels of designing data regulatory frameworks, the amount of data available is extensive. Therefore, considering the scope of this thesis, a selection of relevant regulations and strategies has been necessary. This selection has been done upon considerations of relevance to the overall topic and research question, in which it has been decided to include regulations that informs of both the domestic context – in the case of the EU, regional – and international scope of the different data regulatory frameworks. The selection includes national strategies, laws and regulations, partnerships, as well as other international initiatives.

Specifically, regarding the U.S. case study, the analysis is done upon the official 2017 and 2022 National Security Strategies, the U.S. initiative for enhancement of a transatlantic partnership on cross-border data transfers in the form of the Clarifying Lawful Overseas Use of Data (CLOUD) Act. Regarding the EU case study, analysis will be conducted upon collected material constituting the EU data regulatory framework, here the General Data Protection Regulation (GDPR) framework is essential and will be examined in unison with further EU regulatory implementation, such as the Cybersecurity Act, the Data Act, and the Data Governance Act. While EU member states can have other laws and regulations in place as extension to the GDPR framework, this will not be included in the thesis, as the EU is here included as one collected unit of analysis. Lastly, the EU's legal framework for obtaining digital sovereignty will be included to understand the deeper motivations of the EU's data regulatory framework. Regarding the case study of China's data regulatory framework, the empirical data collected consists of the three main laws constituting the Chinese national data regulatory framework. These are the 2017 Cybersecurity Law (CSL), the 2021 Data Security Law (DSL), and the 2021 Personal Information Protection Law (PIPL). Further, in examining how China holds influence in shaping global data governance, the case study will also include

formal documents on Chinese international initiatives regarding data, such as the Digital Silk Road (DSR), which is to be understood as part of the wider Belt and Road (BRI) infrastructure project.

The three case studies will be further supported by secondary literature directly relating to the included primary sources as well as secondary literature concerning primary events and other initiatives relating to the formation of the three actors' data regulatory frameworks.

Case study analysis with document analysis

Conducting a case study based on three different actors on the topic of global data governance allows for an exploratory analysis of the topic and possibility for further analysis of the complexity of technology and its relevance to international political change. By approaching doing this, the thesis is able to characterise regulations, initiatives, and other events relevant to determining the effect of a fragmented data regulatory framework on global data governance. Further, a case study in the form of three main actors consisting of the U.S., the EU, and China inherently becomes comparative by nature, in that their different approaches will be compared in analysing how they each influence global data governance through various frameworks. This case study comparison includes characterising similarities and differences between the wanted effect of the frameworks, both in their domestic contexts and their extraterritorial effects. Determining the domestic effects is necessary to understanding the intentions of the frameworks, i.e., if they are developed for reasons of security, privacy, or free flow of data. Additionally, by conducting a case study analysis the thesis can comparatively approach how motivations are framed and articulated, such as discursive tools of 'national security' and claiming 'sovereignty.' By also assessing relevant non-state actors and events in leading to the formation of these data regulatory frameworks, the case study analysis can provide the context essential to understanding the fragmented data regulatory framework. Hence, the case study analysis will provide an "in-depth exploration from multiple perspectives of the complexity and uniqueness"[5] of how the different frameworks can influence global data governance.

The foundation for the case study analysis is based on the mentioned data collected in the above section consisting of official documents in the form of strategies, regulations and laws, relevant conceptualisations, and other official documents concerning projects related to the topic of global data governance, from which a document analysis approach is applied.

[5] Starman, Adrijana Biba (2013) "The Case Study as a Type of Qualitative Research." *Journal of Contemporary Educational Studies* vol. 1: 28-43. P. 32.

Approaching the case study analysis from various documents ensures that the information needed for the study can be provided, as the three actors have different approaches to designing their frameworks. Following this necessity, the number of documents collected for the analysis also increased since the beginning of the research process, as "[points] of redundancy"[6] were reached and new insights from additional documents have been necessary to add. Hence, in conducting a fulfilling document analysis it has also been necessary to re-evaluate based on the appropriateness and relevance of the documents selected.

Theoretical considerations

Essentially, constructing first a theoretical overview, then an examination of the three cases of the three key actors – the U.S., the EU, and China – within global data governance, and lastly a theoretical assessment of the cases will help enlighten how the issue of fragmented data regulatory frameworks in global data governance should be examined theoretically. By narrowing the theoretical focus, it will become clearer how to assess issues of technology's impact on and adaptation to politics and society, and vice versa, in examining whether technology should be considered a more important factor in shifting balances of power.

As the theoretical traditions within International Relations are broad, and considering the scope of this project, the theories chosen to first be presented in a theoretical overview and later as theoretical assessments to the case study analysis, have been specifically selected. The selection includes two of the bigger and more dominating theoretical frameworks within IR, those of realism and constructivism, first and foremost, as they will lay a general IR theoretical foundation to later assess the case studies on, in connection with other theories of social science and international politics that centre around technology's influence on spatiality, territory, the global economic system, and public policies. The latter theories will help provide a theoretical foundation upon which the case studies will be analysed, to gain a collected understanding of *why* and *to what effect* the different data regulatory frameworks have been developed in. This selection consists of first, deterritorialisation, a theory that spans across the disciplines of cultural, social, and political studies in its conceptualisation of how globalisation has expanded the possibilities for crossing physical boundaries. Simultaneously with territories being challenged, a process of reterritorialisation happens, in which the concept refers to other territories being drawn, or the active (re)gaining of territory by actors. Second theory in

[6] Morgan, Hani (2021) "Conducting a Qualitative Document Analysis." *The Qualitative Report* 27 (1): 64-77. P. 72.

forming a theoretical analytical foundation is surveillance capitalism, which explains a next level in capitalism dominated by private tech companies, who capitalise on collecting and processing data from its users for behavioural modification gains. Third theoretical framework is the spectrum of techno-nationalism, techno-globalism, and neo-techno-nationalism, in assessing where the actors' regulatory frameworks lead them. This includes considerations of their interactions with the global level in developing policies for technological development, if they are more nationally oriented, or if they balance these two processes more evenly.

Considerations of selecting realism and constructivism as primary IR theories to be included in this thesis, are based upon the two theories understanding of power and how to understand factors that influence power and relations between states. Specifically, realism was chosen as one of the primary IR theories because of its emphasis on power and security, as will be illustrated is relevant to the analysis of this thesis, as the three regulatory frameworks analysed all refer to concerns of security in reasoning the design of their frameworks. Further, considering the context in which these regulatory frameworks are being developed, i.e., great power rivalry and increased global competition in the technological field, a realist perspective on power is useful in analysing the influence of these frameworks in the context of a global fragmented data regulatory framework. Realism will in this regard help in the analysis of frameworks for data governance as approaches by states in (re)gaining power. Considerations on including constructivism surrounds its approaches to identity, norms, and processes of socialisation, and how these theoretically can either help establish data as a vessel of these processes or as a new form of technology that states can utilise for political gain by adding value to it.

Methodological limitations

As this thesis is qualitative in nature from its choices of case studies and documents as primary units of analysis, it inherently has limitations in its approach to the study of global data governance. Three main actors have been chosen to represent what is conceptualised as a fragmented data regulatory framework, which ultimately leaves out various other national and regional frameworks that exists globally. Therefore, it is limited in delivering an analysis framework that could be applied in similar contexts, as these three actors have been chosen specifically on reasons of different frameworks and political and economic significance in international politics. Hence, it does not offer a framework that is necessarily applicable in the

context of smaller powers and regional partnerships. However, determining an overall framework for analysing global data governance in international relations is not the purpose of this study, but rather to approach the subject of a fragmented data regulatory framework as relevant to IR theoretical standpoint and to analytically evaluate how selected IR approaches theoretically assess data and its influence on international politics.

Theoretical Overview

As previously stated, this thesis will first process the various approaches to technology that exist within the greater international relations theoretical traditions. This theoretical overview will contextualise the increased relevance of IR theory to concern itself with theorising technology's impact on international politics by:

- contextualising how the relevant theoretical traditions might lack in their approaches to considering technology as having an increased influence on states
- how states utilise technology to increase power
- and how technological development affect our conceptualisation of power.

This will be done by answering two questions: how does the relevant theoretical frameworks conceptualise power and how technology is conceptualised and considered in connection with power. The various approaches to and conceptualisations of technology is what problematises the study of it in the first place, as articulated by Carr "the complexity is, in fact, the very essence of why we need to study it so carefully."[7]

The theoretical overview will consist of first, two of the more overarching and dominating theoretical traditions within IR, realism and constructivism, in asserting how these theoretical traditions have approached the conceptualisations of power and technology. The choice of these two grander IR theories have been narrowed down specifically to focus the thesis in a more particular manner because of their differing approaches to power and technology. Second part of the overview will consist of an assessment of newer approaches to technology within international politics theory. Considering the scope of this project, choice of newer IP approaches to technology has been particularly selective in order to narrow the focus theoretically to better assess the case study. Specifically, this is focused to include

[7] Carr, Madeleine (2016) *US Power and the Internet in International Relations: The Irony of the Information Age.* Basingstoke: Palgrave Macmillan. P. 21.

deterritorialisation, surveillance capitalism – these two will help contextualise the casework and the reasoning behind states actions to either regulate data or not – and lastly, technological nationalism and technological globalism with their further development of neo-technological nationalism.

Theoretical approaches to technology in international relations

Of the more traditional and still-dominant theories within IR, technology and technological development is typically accounted for as relevant factors in international politics. However, it is often treated as "external to politics, not as something integral to how contemporary politics and world affairs are carried out."[8] While this can be considered a similarity within the dominant IR theories, there are obvious differences as well in their assumptions of power and power balances. To approach their treatment of technology in interrelation with power, I will for starters categorically examine the main IR theories, to including their treatment of key historical events in which technology has been a key driver.

Realism

As a defining dominating theory of IR, realism, with its many variations, have been essential in trying to define power and how power is obtained. Within realism, nation states act as the primary actors within an international system that is rooted in an anarchic structure – that is, an international system without any governing authority over sovereign states, leaving states to compete for power. In its different variations, realist scholars have attempted to define power as a concept together with why states as the main actors fight for power. The classical realist Hans J. Morgenthau argues in his *Politics Among Nations* and the later added 'Six Principles of Political Realism' that "politics, like society in general, is governed by objective laws that have their roots in human nature."[9] Morgenthau carries a historic approach to the subject of power and assumes from this "that statesmen think and act in terms of interest defined as power,"[10] but that national interest and motivations for political action is not fixed but dynamic since it "depends upon the political and cultural context within which foreign policy is

[8] Eriksson, Johan and Lindy M. Newlove-Eriksson (2021) "Theorizing Technology and International Relations: Prevailing Perspectives and New Horizons." In *Technology and International Relations: The New Frontier in Global Power* 3-22, ed. Giampiero Giacomello, Fransesco N. Moro and Marco Valigi. Cheltenham: Edward Elgar Publishing. P. 5.
[9] Morgenthau, Hans J. (2005 [1948]) *Politics Among Nations*. Seventh Edition revised by Kenneth W. Thompson and W. David Clinton. Boston: McGraw-Hill. P. 4.
[10] Morgenthau 2005, 5.

formulated."[11] Since interest is defined as power, Morgenthau applies this to the concept of power as well, as "its content and the manner of its use are determined by the political and cultural environment," while emphasising his assumption in political action and the quest for power being rooted in human nature as "power covers all social relationships […] by which one mind controls another. Power covers the domination of man by man, both when it is disciplined by moral ends and controlled by constitutional safeguards."[12] The classical realism belief of states' drive to seek out power as being rooted in human nature is later challenged by the coming of structural realist, also called neo realist. Structural realists concur with classical realists' notion of states being the main actors in the international system and ultimately motivated by obtaining power. However, they differ in the belief of states' power-seeking behaviour being rooted in human nature, as structural realist rejects this notion. Instead, structural realists focus on the power distribution in the international system. As according to structural realist Kenneth Waltz, the distribution of power affects states' behaviour as states become aware of how other states might utilise their power to benefit their national interests. This consequentially leads to worries of security and one's security being threatened by other states amount of power. Hence, in Waltz' structural realism, security becomes a primary focus for states and states seek to enhance security in order to defend themselves, leading to the term of defensive realism for Waltz' position.[13]

In contrast to Waltz, John Mearsheimer builds the theoretical position of offensive realism in his *The Tragedy of Great Power Politics*. Mearsheimer agrees with the defensive realist reasoning of states being concerned with power as a means of security and survival in an anarchical international system but criticises Waltz' approach to states and power as status-quo powers. Instead, as per Mearsheimer, states, and specifically great powers, will always seek optimization of power to ensure security, which entails offensive rather than defensive traits, because of the structure of the anarchic international system. As Mearsheimer states in his book "a state's ultimate goal is to be the hegemon in the system," hence, great powers, in his realist notion, are always incentivised to optimise power.[14] The last main addition within realist thinking is the neoclassical realist framework, which is concerned with including the domestic context to international power struggles. Neoclassical realism combines classical and

[11] Morgenthau 2005, 11.
[12] Ibid.
[13] Dunne, Tim and Brian C. Schmidt (2014) "Realism." In *The Globalization of World Politics: An Introduction to International Relations*, Sixth Edition, 99-112, ed. by John Baylis, Steve Smith and Patricia Owens. Oxford: Oxford University. P. 105.
[14] Mearsheimer, John J. (2001) *The Tragedy of Great Power Politics*. New York: W. W. Norton. P. 21.

structural realism in its approach to understanding why states compete for power in the international system. Within neoclassical realist thinking, the domestic process is important in considering foreign power struggles, since various factors such as state leaders, state-society relations, and state identity also influences foreign policy outputs. Hence, within neoclassical realist thinking the distribution of power in the international system as well as the domestic context is important. As identified by Gideon Rose, "power analysis must therefore also examine the strength and structure of states relative to their societies, because these affect the proportion of national resources that can be allocated to foreign policy."[15]

Regarding the influence of technology and technological development on international politics, realism tends to consider technology as a secondary factor to the primary factors of security and material power, which matters to states the most. As a secondary factor, "technology is traditionally regarded a 'force multiplier,' or more generally as belonging to the category of 'material capabilities' of states."[16] An area in which realists acknowledge technology's influence is from its contributions to technologies of communication, surveillance, and military value, and how technology in these areas can help gain superiority.[17] One specific technology that has gained a lot of attention from realists is nuclear weapons, which serves as an example of how realist "claim that the distribution of technological capacity can have pivotal effects on the balance of power, and thus on whether there is stable peace or heightened risk of war,"[18] while also conceptualising nuclear deterrence, in which distribution of nuclear weapons between countries can have an effect of de-escalation because of the possibility of nuclear retaliation. However, despite nuclear weaponry being an example of one technology gaining plentiful traction in realist scholarship, realists generally maintain that technology does not hold the relevant influence that can challenge or "change the nature of international relations."[19] Thus, technology merely holds a position of a secondary factor that might help gain superiority in certain aspects, but while "technology may change, and technology may also impact on international relations, […] the nature of politics remains essentially the same."[20]

[15] Rose, Gideon (1998) "Review: Neoclassical Realism and Theories of Foreign Policy." *World Politics* 51 (1): 144-172. P. 147.
[16] Eriksson and Newlove-Eriksson 2021, 6-7.
[17] Eriksson and Newlove-Eriksson 2021, 7.
[18] Ibid.
[19] Ibid.
[20] Ibid.

Constructivism

The constructivist theoretical framework seeks to both critique realism's and liberalism's approach to power but also to fill out the gap left behind by these two aforementioned theoretical frameworks. Constructivist do not critique what realist and liberalist say and do but rather what they ignore of "the content and sources of state interests and the social fabric of world politics."[21] Constructivism's relationship with realism and liberalism "is complementary, not competing," as argued by Martha Finnemore.[22] Thus, constructivists also consider the international structure as important, but chooses to focus on meaning and social value within the international structure. This is because all states are inherently a part of a dense global network of social relations, which "shape their perceptions of the world and their role in that world. States are *socialized* to want certain things by the international society in which they and the people in them live"[23] (emphasis added in the original). What shapes behaviour of states is inherently interest in constructivist thought, hence, constructivist aim to examine what shapes the interests of states. Constructivism focuses on the importance of ideas, norms, and identity in shaping the behaviour of states through their interests and their relations with one another. When concerning the notion of norms within constructivist thinking, it is to be understood as collective meaning or understanding, which constitutes the norms of states. These collective meanings are shared between states in what Alexander Wendt phrases as the "distribution of knowledge," which is what ultimately affects how states perceive the distribution of power. Hence, Wendt argue that "it is collective meaning that constitute the structures which organize our actions."[24] This argument is further shared by Finnemore, who argues that material and economic conditions are not all to be observed within the structure of the international system but that "structures of shared knowledge and intersubjective understandings may also shape and motivate actors."[25] Further, it is the intersubjective understandings and shared knowledge, which form norms concerning "shared expectations about appropriate behavior held by a community of actors."[26] Wendt believes that it is the

[21] Checkel, Jeffrey T. (1998) "Review: The Constructivist Turn in International Relations Theory." *World Politics* 50 (2): 324-248. P. 324.
[22] Finnemore, Martha (1996) "Defining State Interest." In *National Interests in International Society*, 1-33. Ithaca: Cornell University. P. 26-27.
[23] Finnemore 1996, 2.
[24] Wendt, Alexander (1992) "Anarchy is What States Make of it: The Social Construction of Power Politics." *International Organization* 46 (2): 391-425. P. 397.
[25] Finnemore 1996, 15.
[26] Finnemore 1996, 22.

active participation in collective meanings that then shapes actors' (states) identities or that they can acquire identities through participation, as "identities are inherently relational."[27] After acquiring identities from participating in collective meanings, actors participating in said collective meaning tend to follow each other in their practices, which Wendt describes as "the symbolic interactionist notion of the 'looking-glass self,' which asserts that the self is a reflection of an actor's socialization."[28] It is further also possible for states to influence internationally through interactions of various degree, by implementing their held norms through processes of socialisation. So, through a constructivist lens, states interests are formed on the basis of the collective meanings that they participate in, which shapes their norms and identities, together with how they view other states, i.e., friend or foe or in between.

Concerning constructivism's consideration of technology and technology's influence on international politics, it is perhaps appropriate to start with the infamous example of nuclear weapons, as illustrated by Wendt. The example goes that the U.S. would find five hundred UK nuclear weapons less threatening than five North Korean nuclear weapons "because of the shared understandings that underpins them," based on the meaning attributed to forces of destruction are "the '*relations* of destruction' in which they are embedded"[29] (emphasis added in the original). Hence, a constructivist framework assumes materialist matters in a light of the already constructed identities and shared meanings between states, and thus "constructivism suggest that material forces must be understood through the social concepts that define their meaning for human life."[30] Hence, constructivism's view of technology differs from that of realism, as constructivism does not, in the case of nuclear weaponry, concern itself with gains and material capacity but rather how states share meanings and identities through the object of nuclear weaponry.[31] This essentially portrays well a general constructivist approach to technology's role and influence on international political change – technology is neutral in its form and effect, therefore "it is what actors make of it, and in this sense it is 'politically neutral,' or rather possible to politicize in many different ways."[32]

[27] Wendt 1992, 397-398.
[28] Wendt 1992, 404.
[29] Wendt, Alexander (1999) "Three Cultures of Anarchy." In *Social Theory of International Politics*, 246-312. Cambridge: Cambridge University. p. 255.
[30] Hurd, Ian (2008) "Constructivism." In *The Oxford Handbook of International Relations*, 298-316. Edited by Christian Reus-Smith and Duncan Snidal. New York: Oxford University. p. 301.
[31] Eriksson and Newlove-Eriksson 2021, 11.
[32] Ibid.

Deterritorialisation

Deterritorialisation has its roots as a political-philosophical concept by Gilles Deleuze and Félix Guattari in their writings wherein they explain the workings of shifting subjectivities under capitalism.[33] Deterritorialisation and its twin concept of reterritorialisation are processes of territorialisation that happens simultaneously. Deterritorialisation has since become a widely used conceptual and theoretical framework in social, cultural, and political theory, particularly within studies of globalisation and modernisation. Within a cultural studies approach, a key focus of deterritorialisation is particularly how it is a process of breaking down territorial boundaries. Arjun Appadurai argues in his 1990 *Disjuncture and Difference in the Global Cultural Economy* that deterritorialisation occurs in context with globalisation and cultural exchange. Appadurai explores this through five dimensions of cultural flows that he coins ethnoscapes, mediascapes, technoscapes, finanscapes, and ideoscapes, in which global cultural flows occur "*in and through the growing disjunctures between* [the five dimensions]" (emphasis added in the original) and that "the sheer speed, scale and volume of each of these flows is now so great that the disjunctures have become central to the politics of global culture."[34] With this, Appadurai refers to a deterritorialisation that pertains to breaking down of traditional territorial and cultural boundaries and the emergence of new cultural flows, which are important of our understanding of change in the global cultural economy and the digital age.

Further, deterritorialisation refers to a process of transformation of social relations in the changing state of territorial, cultural, and social boundaries. This is a recurring process in Manuel Castells' book *The Rise of the Network Society*, in which Castells explores a new form of social organisation that he terms the network society. He argues that because of communication networks, social relations are shifting away from the more traditional ways of social organising through physical and territorial boundaries towards communication networks instead. This creates a process of deterritorialisation that is driven by the emergence and rapid increasing of global communications networks, wherein new forms of social and economic activity take shape beyond the traditional physical boundaries.[35] As stated, in the process of deterritorialisation, reterritorialisation happens simultaneously as it refers to a process of

[33] Lambach, Daniel (2020) "The Territorialization of Cyberspace." *International Studies Review* vol. 22: 482-506. P. 491.
[34] Appadurai, Arjun (1990) "Disjuncture and Difference in the Global Cultural Economy." *Theory, Culture & Society* vol. 7: 295-310. P. 301.
[35] Castells, Manuel (2010 [1996]) *The Rise of the Network Society*. Second Edition. Chichester: Blackwell. P. 502.

"restructuring or reconstitution of social relations in some other territorial form."[36] Lambach illustrates this process by referring to globalisation as a process of deterritorialisation in which "the disembedding of economic and financial relations from their territorial foundations are the results of political choices and technological development."[37] Using cyberspace as example of a deterritorialised space within the process of globalisation, Lambach further explains how a process of reterritorialisation occurs simultaneously by states and corporations reacting to the deterritorialisation by viewing "cyberspace as something to be controlled, regulated, and exploited. Such visions, narratives, and discourses are not just speech acts but *at the same time* attempts at (re-)territorializing cyberspace"[38] (emphasis added in the original).

Following the case studies conducted in this thesis, the theoretical assessment will examine if the rapid digital technological development can explain a process of deterritorialisation, and how this might be understood as cause and reasoning behind the various data regulatory frameworks that are being developed, i.e., the fragmented data regulatory framework experienced globally.

Surveillance capitalism

Following the presentation of deterritorialisation, another relevant approach of understanding how technology travels across borders and challenges political realities, is that of surveillance capitalism, an approach to understanding how technology is challenging and transforming our day-and-age by Shoshana Zuboff in her book *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Through the framework of surveillance capitalism, Zuboff examines the growing power and impact that major technology corporations hold in a new global economic system by collecting and analysing data from users globally. Zuboff bases her analysis on major corporations like Google and Facebook, which collects and processes data from its users to target advertising and other services, because of data's increased importance as an asset in the digital economy. This economic system, built around harvesting and processing data, is the essence of surveillance capitalism. Zuboff argues that companies like Google and Facebook's decision to use data in this way becomes a means of power and influence over our lives, in that their collection and utilisation of our data have the means to affect and change our behaviour. She argues that this is an occurrence from the

[36] Lambach 2020, 492.
[37] Ibid.
[38] Ibid.

general shift of how data is handled after being collected – beforehand the purpose of collecting data was to better the services for the direct users, where now it is instead not just predicting what we might need but deciding it, as formulated by Zuboff, "it is no longer enough to automate information flows *about us*; the goal is now to *automate us*"[39] (emphasis added in the original). It is the behavioural modification aspect of surveillance capitalism that Zuboff considers a new form of power, which she coins instrumentarian power that "knows and shapes human behavior toward others' ends. Instead of armaments and armies, it works its will through the automated medium of an increasingly ubiquitous computational architecture of 'smart' networked devices, things, and spaces."[40] Zuboff further extends that the players of the surveillance capitalist market will only continue to intensify their "means of behavioral modification and the gathering might of instrumentarian power," because the history of industrial capitalism tells us this, only with the change of means of production to means of behavioural modification in this instance.[41]

Techno-nationalism, techno-globalism, and neo-techno-nationalism

The last approaches to the study of technology and its global influence that will be explained in this brief overview is the oppositional approaches of techno-nationalism and techno-globalism and the intertwining process of combining these two under the approach of neo-techno-nationalism. The first, techno-nationalism, is an approach used to describe the process in which domestic policies are formed to target specific domestic industries in an effort to enhance their performance, often industries within technological development. A part of this process involves providing governmental support to the specific industries through giving "government procurements, import restrictions, export subsidies, research and development (R&D) subsidies, R&D tax credits, controls on inwards foreign direct investments, protection of intellectual properties, government-funded R&D projects."[42] When analysing technological development through a techno-nationalist approach, the key unit of analysis is the nation, meaning "nations are the units that innovate, that have R&D budgets and cultures of innovation, that diffuse and use technology," hence "[t]he success of nations […] is dependent on how well

[39] Zuboff, Shoshana (2019*) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books. P. 8.
[40] Ibid.
[41] Zuboff 2019, 9.
[42] Yamada, Atsushi (2000) "Neo-Techno-Nationalism: How and Why It Grows." Working Paper for *International Studies Association Convention*, March 14-18, 2000 - https://ciaotest.cc.columbia.edu/isa/yaa01/

they do this."[43] Thus, techno-nationalism assumes that through targeting public policy to support specific domestic technological industries, it is the national government that "lead[s] the direction of innovation."[44] In contrast to techno-nationalism, techno-globalism is concerned with the globalising aspect of technological development. Theoretically and ideologically, techno-globalism follows the practicalities of globalisation in considering technology and technological development as a vessel for connecting the world. This approach argues that various of the key technological developments – the radio, the aeroplane, and information communication technologies – that have been developed nationally but shaped and connected us globally by "forging a new global world economy and culture," meaning that techno-globalism holds a view that "nations is at best a temporary vehicle through which the forces of techno-globalism operate but are always about to disappear through the advance of globalizing new technology."[45]

As simple as these two frameworks seem to be in their theoretical and ideological worldviews as opposing one another, David Edgerton criticises the contradicting issues they represent in their historical and geopolitical foundations as missing critical factors that have influenced technological development. The critique especially concerns a conflation of the 'national' and the 'global' as strictly two distinct units of analysis instead of an interrelated process. An example of this that Edgerton presents is techno-globalist's tendency to defend their position using examples of major technological developments, as for example aviation and telecommunication, as having altered global society. Edgerton points out how these technologies have been developed with nationalist goals and purposes in mind, e.g., the radio "which had a military origin, was intimately connected to national power."[46] As already referenced, techno-globalist view the nation as a vessel which techno-globalism operates through, however, Edgerton criticises this notion as he argues that many of the twentieth century technologies that techno-globalist views as internationalising are actually created within specific state systems that could not have thrived globally from the offset as a lot were "technologies of autarchy and militarism."[47] Concerning this mindset of erasing the national from techno-globalist operations, Edgerton argues that a lot of these technologies "were the product of the particular state system which operated to force nations into particular relations

[43] Edgerton, David (2007) "The Contradictions of Techno-Nationalism and Techno-Globalism: A Historical Perspective." *New Global Studies* 1 (1): 1-32. P. 1.
[44] Yamada 2000 - https://ciaotest.cc.columbia.edu/isa/yaa01/
[45] Edgerton 2007, 1.
[46] Edgerton 2007, 13.
[47] Edgerton 2007, 14.

with each other. The very specific role of the state, and the specific nature of its competition with other states has given *states* particular roles in the promotion of *particular* technologies" (emphasis added in the original).[48] Concerning techno-nationalism, Edgerton emphasises how techno-nationalist approaches to technological development historically have, because of geopolitical factors, also been essential within autarchic state structures, with states trying to lead technological and political boundaries in line with one another, despite their boundaries being different. However, as he points out "this practical technological nationalism has had wonderfully contradictory effects – far from making national technologies different, it has encouraged movement of technologies across political boundaries" because these techno-nationalist structures would be unable to meet the demand for the technology required, and that it "also helped impoverish nations rather than strengthen them."[49] In general, Edgerton criticises both techno-nationalism and techno-globalism for their simplicity in explaining what drives technological development affect the national and global levels. Specifically, he emphasises how "politics, multinational firms, empire and race were also crucial factors in shaping the use of technology which cut across the national and global divide in complex and changing ways,"[50] hence, merely focusing on technological development within a scope of national or global society overlooks many nuances.

Having presented techno-nationalism and techno-globalism, the last framework for how we can examine technological development is through the neo-techno-nationalist framework, as proposed by Atsushi Yamada. Yamada argues that "the conventional dichotomy of techno-nationalism and techno-globalism […] is inadequate for a better understanding of the changing nature of all major nations' technology policy today."[51] Yamada proposes neo-techno-nationalism as combining aspects of techno-nationalism and techno-globalism by recognising that these two frameworks each on its own has shortcomings that cannot quite explain the global and national structure wherein technology policy is being developed and for what purpose. Neo-techno-nationalism instead assumes the global and local levels as being interlinked, with some policies being developed from national concerns and others in accordance with the global structure. Techno-nationalist policies can be developed because of political concerns of domestic industries, and a techno-globalist focus because of economic

[48] Ibid.
[49] Edgerton 2007, 15.
[50] Edgerton 2007, 1.
[51] Yamada 2000 - https://ciaotest.cc.columbia.edu/isa/yaa01/

rationale. It can also be understood as "techno-nationalism grows when a nation faces severe competition with foreign rivals, while techno-globalism flourishes during an economic boom."[52] The development of a neo-techno-nationalist framework seems to very much having been in accordance with the real-world development of rapid digital technological development and is hence not a set dichotomy of the two contradictions of nationalism and globalism that states can just switch between according to their political needs. Instead, it should be understood as "a hybrid that consists of the elements complimenting each other."[53] Yamada argues that this hybrid – neo-techno-nationalism – is a "response to the ongoing glocalization of technology," where states will form neo-techno-nationalist policies "to meet the challenges posed by glocalization and advance their own national interests in a 'glocalized' economy."[54] The practical steps of this includes both steps of promoting domestic technological innovation, a bigger emphasis on public-private partnerships, increased possibility for foreign R&D investment, and further international cooperation on policy coordination, as according to Yamada's four main characteristics of neo-techno-nationalism. Hence, the neo-techno-nationalist approach follows that much technological innovation and development arises from the private sector, but the state does not withdraw itself from the process, they instead emphasise an increased importance of the public and private sectors working together, while still acknowledging the relevance of foreign input to one's technological development and actively partaking in international rulemaking.[55] Therefore, Yamada's proposition of neo-techno-nationalism "does not intend to prevent the global flow of technology […] [instead] it aims to leverage globalization" but "its goal is to advance national interests, rather than global interests, by promoting localization and promoting further innovation that will be even more crucial for economic growth and prosperity in the 21st century."[56]

From this theoretical overview various approaches to examining technological development in relation to international politics have been presented. Like most subjects, there are various theoretical approaches to analysing technological development's influence on international politics, yet it is also clear that most of the approaches lack a fully formed foundation upon which such analysis can be done. As Edgerton exclaims, "the nation, the state, and the global, are central to the history of twentieth-century technology, but not in the ways the relations are

[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Ibid.

usually understood. We need to rethink not only nation-technology, but technology-state relations, and the place of technology at a global level too."[57] It is from this offset that the thesis will precede, following the case-study analysis, by combining several theoretical approaches to create a more holistic foundation for further analysis. This thesis does not aim to propose a new theoretical approach to the subject but rather to examine how the theories presented might be able to engage more broadly with one another in order to understand the complicated process of the subject better.

Case study analysis

Global data governance involves several levels of actions and participation in which national and regional policy making is one of them but just as important is the outreach and influence that these policies hold. Further, states participation in the international system through targeting and influencing of international standardisation is where states can create leeway for their own positions and approaches but also gain power through influencing the international order. Lastly, the role of major multinational tech corporations has been foundational in the formation of how data has been handled and still is, in many parts causing friction because of how states and regions choose to respond to their influence.
When examining the three actor's data regulatory frameworks, it is naturally relevant to note their difference in creation of data regulations, be it based on state, national, and regional levels, as well the relevance of combining both regulations focused on domestic and foreign circumstances. While the focus in examining the fragmented data regulatory frameworks in connection with global data governance will be more on how the relevant actors essentially differ or align on data transfers, each domestic context is necessary to include in order to gain a more holistic understanding of their data policies.

When considering data regulations in international politics, this thesis understands it as a tool of precaution more than a technological initiative by itself. It falls under the realm of technological initiatives and can be conceived as a variety of motivations in designing the different policies, but with the significant rise in digital technological development, the competition it brings with it, and security threats that it poses, the data regulatory frameworks

[57] Edgerton 2007, 1.

designed by major powers can do both, but they mainly emphasise security, be it personal or national. Hence, while the actual different national and regional policies are core elements to understand by themselves, they can in the context of understanding global data governance not stand isolated, within this context both states and corporations' participation in and influence on the formulation of international standard-setting is just as important to analyse as how data is governed globally. Likewise, national and global industry growth and how states support this, are incredibly important in examining global data governance, considering the dominance of intellectual property rights in being able to access and maintain domination within key industries and global markets.

The U.S.

The U.S. data regulatory framework expands across a wide variety of national and state laws and regulations but with no overreaching national data laws set in place. At the federal level, the laws and regulations are specifically aimed at various sectors and covers "financial institutions, telecommunications companies, credit reporting agencies and healthcare providers, as well as driving records, children's privacy, telemarketing, email marketing and communications privacy laws."[58] However, laws of privacy and data protection are mostly initiated and implemented on state levels, with California being an example of a state with a wide privacy and data security regulations set in place, the most comprehensive one being the California Consumer Privacy Act, which allows citizens of California to have more control over their personal information such as a right to know what data has been collected about them and the right to have it deleted.[59] More U.S. states are following California in implementing data security regulations but California's data regulatory framework remains the most comprehensive regarding options of personal information protection.[60] With U.S. data and privacy laws varying greatly across the national and state levels, assessing a complete U.S. approach to data regulation is ultimately complex, but regarding collection of data, U.S. data regulation "generally require that a notice be provided or made available pre-collection […]

[58] Data Protection Laws of the World (2023) "United States: Law." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?c2=&c=US&t=law
[59] State of California Department of Justice (2023) "California Consumer Privacy Act (CCPA)." February 15, 2023. Accessed April 15, 2023 - https://oag.ca.gov/privacy/ccpa
[60] Data Protection Laws of the World 2023, https://www.dlapiperdataprotection.com/index.html?c2=&c=US&t=law

that discloses a company's collection, use and disclosure practices, the related choices individuals have regarding their personal information, and the company's contact information."[61] Further, if a company wishes to utilise the collected data in different ways from what has been informed when the data was collected, they will need to "obtain opt-in consent prior to using, disclosing or otherwise processing personal information in a manner that is materially different than what was disclosed in the privacy policy applicable."[62] Regarding security of personal information collected from U.S. citizens it again varies greatly depending on state laws and regulations, as there are not general national regulations, however, "most U.S. businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information."[63]

U.S. National Security Strategies and data

Generally, most U.S. laws and regulations on data are concerned with healthcare, financial data, and consumer privacy and much less concerned with cross-border data flows. According to Data Laws of the World, the U.S. has no laws specifically concerned with transfer of data across geographic territories "except regarding the storing of some governmental records and information,"[64] they have, however, completed strategies and other initiatives to control data transfers. First, the U.S. government has emphasised the various ways in which data is important through different strategies under different administrations. In both the 2017 National Security Strategy, from the Trump administration, and the 2022 National Security Strategy, from the Biden-Harris administration, data is frequently mentioned as essential to further the development and security of the digital economy, development of critical infrastructure, and safeguarding of information and privacy. In the 2017 National Security Strategy, data is first highlighted as a key element in accessing information to which other competitions are accelerated – economic, political, and military – as articulated, "the ability to harness the power of data is fundamental to the continuing growth of America's economy, prevailing against hostile ideologies, and building and deploying the most effective military in

[61] Data Protection Laws of the World (2023) "United States: Collection and Processing." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?c2=&c=US&t=collection-and-processing
[62] Ibid.
[63] Data Protection Laws of the World (2023) "United States: Security." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?t=security&c=US
[64] Data Protection Laws of the World (2023) "United States: Transfer." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?t=transfer&c=US

the world."[65] The vulnerability of data is further articulated as being a target of foreign powers,[66] and that data is to be protected along with the networks they are in to remain secure. How to do so is not further specified here, other than to "encourage practices across companies and universities to defeat espionage and theft."[67] Another key representation in the strategy is data emphasised as being of main importance in modern weapons system since these "depend upon data derived from scientific and technical intelligence."[68] In the 2017 strategy, data is generally emphasised as strategic asset to ensure national security and competition.[69] Lastly, the strategy highlights that the free flow of data – in unison with a free and open internet – is essential in ensuring "the success of the U.S. economy."[70]

The 2022 National Security Strategy links the importance of data together with technology and technological development as essential to keeping up with if the U.S. is to maintain its role in the international system and as key actor in shaping the rules of the international world order. As articulated in the strategy, "we are endeavoring to strengthen and update the UN system and multilateral institutions generally. Nowhere is this need more acute than in updating the rules of the road for technology, cyberspace, trade, and economics."[71] A part of this is to continue investments in several industries of technological development, as well as research and development, cooperating with "allies and partners to harness and scale new technologies, and promote the foundational technologies of the 21st century."[72] It is through cooperation with like-minded partners that the strategy sees opportunities for "promot[ing] the free flow of data and ideas with trust, while protecting our security, privacy, and human rights, and enhancing our competitiveness" and hopes to "close regulatory and legal gaps, strengthen supply chain security, and enhance cooperation on privacy, data sharing, and digital trade."[73] Like the 2017 strategy, the 2022 strategy also underlines how data functions as an asset that can be exploited by foreign powers – or, as articulated, 'strategic competitors' – which can threaten American security. To counter this, the strategy suggests that "to achieve

[65] The White House (2017) "National Security Strategy of the United States of America." *Trump White House Administration*, 1-55 - https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf. P. 3.
[66] The White House 2017, 14.
[67] The White House 2017, 22.
[68] The White House 2017, 32.
[69] The White House 2017, 34.
[70] The White House 2017, 40.
[71] The White House (2022) "National Security Strategy." *Biden-Harris White House Administration*, 6-48 - https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf. P. 32.
[72] The White House 2022, 33.
[73] Ibid.

these goals, the digital backbones of the modern economy must be open, trusted, interoperable, reliable, and secure," which should be achieved through cooperating with partners on "network infrastructure resilience in 5G and other advanced communication technologies, including by promoting vendor diversity and securing supply chains."[74] To summarise, both strategies developed under different administrations highlight similar aspects to the importance of data and provide clear ideas on how data should be controlled and regulated. First, data is considered a strategic asset that can be exploited for benefit by other powers, hence it becomes valuable to secure in order to ensure national security. Second, data is continuously emphasised as being connected to the modern digital economy and economic development, through emphasis on data's importance on global supply chains and trade. Because of the strategies emphasis on this, they both repeatedly articulate the need for ensuring a free flow of data and data sharing to enhance the economy. Again, this is linked with national security in both strategies, hence, the vitality of data is being interlinked with trade, economic enhancement, and national security.

U.S. influence on global data governance

Other U.S. initiatives to regulate data outside of just a national context include the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act, as well as the U.S.'s efforts to advocate continuation of free flow of data through "upholding existing agreements within the WTO framework […] [since] data localization is likely to be in violation of the General Agreement on Trade in Services (GATS)."[75] This can however be disputed, as Lin argues, because the GATS also has exemptions for some scenarios where data localisation is justified if necessary to comply with laws and regulations in order to secure protection of private information.[76] It does however, emphasise how the U.S views the free flow of data as being critical, as the U.S. continuously advocate it through various channels of alliances, partnerships, international organisation and standardisation, and through their own regulatory initiatives, such as the CLOUD Act. The CLOUD Act was enacted to "speed access to electronic information held by U.S.-based global providers that is critical to [U.S.] foreign partners' investigations of serious crime,"[77] and is further described to function as a tool for U.S. partners with strong privacy and

[74] The White House 2022, 33-34.
[75] Lin, Xiaofeng (2020) "A Dangerous Game: China's Big Data Advantage and How the US Should Respond." *Journal of Law, Technology and Policy* vol. 2020 no. 1: 253-281. P. 280.
[76] Ibid.
[77] The United States Department of Justice (2018) "CLOUD Act Resources." Updated March 8, 2023. Accessed April 15, 2023 - https://www.justice.gov/criminal-oia/cloud-act-resources#:~:text=The%20CLOUD%20Act%20is%20designed,fight%20serious%20crime%20and%20terrorism.

data regulations to obtain necessary information when needed in investigatory work. The CLOUD Act is proposed to offer new opportunities for U.S. trusted foreign partners through bilateral agreements to obtain information otherwise stored in the U.S. or another country, which will "make both nations' citizens safer, while at the same time ensuring a high level of protection of those citizens' rights."[78] Because of the nature of the CLOUD Act and its promotion of bilateral agreements, it has raised issues of worry among some of the U.S.'s trusted foreign partners, here among the EU. Therefore, further examination of the CLOUD Act in combination with U.S.-EU transatlantic partnership will follow later on, after a look into the EU's data regulatory framework. First, however, it is relevant to examine other ways in which the U.S. has shaped global data governance.

As a leading power, the U.S. approach of promoting a rather techno-libertarian approach to digital data stand in close connection to the liberal free market approach. This approach has been dominating with its ideological approach to free flow of data, which has essentially been to accommodate U.S. tech companies and served as a major advantage for these companies to grow as they have and dominate the global tech market. The U.S. has thus enjoyed large economic value from data flows more than anybody else from the so-called Silicon Valley Consensus, the "belief that technological change leads to economic prosperity for individuals, cities, regions and states."[79] The Silicon Valley Consensus can be understood as consisting of principles, which guide U.S. data governance. These principles are the "free flow of data, prohibition of data localization and a basic level of data protection."[80] Thus, creating a domestic environment and promoting a global environment, where data can flow freely has been essential in U.S. data governance. Further, major Silicon Valley tech companies hold political power to such a degree that they have tried to influence U.S. international data policy involvement, by trying to get the "U.S. government to limit the role of the International Telecommunications Union […] so that tech companies could operate with as little regulation as possible."[81] In addition to this, the U.S. advocates the interests of its major tech companies, such as by criticising the EU and the UK for digital taxes, by arguing that the "tax schemes

[78] Ibid.
[79] Nussipov, Adil (2020) "Data Governance in America: Between the Silicon Valley Consensus and California's Privacy Rules." *Center for Media, Data and Society*, February 10, 2020. Accessed April 10, 2023 - https://medium.com/center-for-media-data-and-society/data-governance-in-america-between-the-silicon-valley-consensus-and-californias-privacy-rules-f78cb8619008
[80] Ibid.
[81] Okumus, Serra (2022) "The Rising Political Power of Silicon Valley." *Fiker Institute*, April 2022. Accessed April 10, 2023 - https://www.fikerinstitute.org/publications/the-rising-political-power-of-silicon-valley

[are] designed to unfairly target [U.S.] companies."[82] A last point to be remarked here, is that while the U.S. does not have strict data regulations, like its counterparts in the EU and China, and instead promotes the free flow of data with limited restrictions, the U.S. does still take counter measures, where it sees it fit. Rather current examples of this are the U.S. effort to first pursuing regulation of TikTok to now attempting to have it sold to an American company, as well as U.S. sanctions on Huawei. The controversy surrounding TikTok in the U.S. (and other countries) is one of 'platform politics,' as argued by Gray, in which TikTok becomes a subject in geopolitical tensions between the U.S. and China.[83] Regarding Huawei, the U.S. has taken extensive measures to curb Huawei from competing with U.S. tech companies, such as export controls on Huawei suppliers and banning export of semiconductors.[84]

U.S. influence on global data governance is formed through dominance in digital technological innovation, legal and regulatory frameworks – such as the Transatlantic Partnership – and international standard setting. Through these various channels, the U.S. promotes the free flow of data, which specifically favours U.S. dominance on digital technological development and the digital economy, while also adding a national security aspect to their data governance approach by limiting e.g., Chinese companies in their competition with U.S. companies.

The EU

The European Union is regarded as having one of the strongest data and privacy frameworks, which is specifically focused on the notion of the 'right to be forgotten,' which then centres EU citizens privacy as the main aspect to be protected. Different variations of regulations and notions of the 'right to be forgotten' has been present in Europe for several decades but was officially included as a proper right after a 2014 court case, when the EU Court of Justice ruled against Google Spain in a case of whether an individual could have data about them collected by Google deleted. Specifically, the case concerned Costeja Gonzalez, who wished to have

[82] BBC (2020) "US Challenges 'Unfair' Tech Taxes in the UK and EU." *BBC News*, June 2, 2020. Accessed April 10, 2023 - https://www.bbc.com/news/business-52896266

[83] Gray, Joanne (2021) "The Geopolitics of 'Platforms': the TikTok Challenge." *Internet Policy Review* 10 (2): 2-26. P. 8.

[84] Kawakami, Takashi et al (2023) "Huawei's Rebirth as Cloud Provider Faces Total U.S. Export Ban Threat." *Nikkei Asia*, March 3, 2023. Accessed April 10, 2023 - https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-rebirth-as-cloud-provider-faces-total-U.S.-export-ban-threat#:~:text=The%20U.S.%20Commerce%20Department%20first,government%20could%20access%20sensitive%20data.

links to an article about him deleted by Google, since he could not have the article itself taken down. Google Spain sent his request on to Google Inc. in the U.S., but Google did not wish to fulfil his request.[85] The case sparked a wider legal discussion around when an individual is able and have the right to demand their data deleted. The European Court of Justice ended up deciding that a search engine is regarded as a 'controller,' meaning that they bear the responsibility to safeguard personal data in their processing, and that in this specific instance "operators of search engines can be required to remove personal information published by third party websites."[86] Further, the notion of 'the right to be forgotten' is discussed as well, because some, like Lynskey, argue that it is too often conflated with 'the right to erasure,' which is essentially what became the result of the Google Spain court case. Lynskey argues that there are differences between these two notions by making the distinction between practical processing and personal references, hence saying they should not be conflated.[87] However, 'the right to be forgotten' and the 'right to erasure' are referenced together under Article 17 in the GDPR.[88] Following the introduction of the 'right to be forgotten' or 'right to erasure,' the following sections examine the EU's approach to designing a comprehensive data regulatory framework, which is heavily based around the introduction of the GDPR framework, as well as various other regulatory implementations, and the notion of 'digital sovereignty' as instructing basic principles and policy initiatives to digital technological development and data protection.

The GDPR framework

The GDPR was adopted in 2016, went into effect in 2018, which replaced the former 1995 Data Protection Directive, and is a legislation which sets out to protect all EU citizens' privacy and personal data, meaning the protection of the "processing of personal data and rules relating to the free movement of personal data."[89] The law is substantial in its approach to the protection

[85] Lynskey, Orla (2015) "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez." *The Modern Law Review* 78 (3): 522-548. P. 523.
[86] Global Freedom of Expression (na) "Google Spain SL v. Agencia Espanola de Protección de Datos." *Columbia University*. Accessed April 14, 2023 - https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/
[87] Lynskey 2015, 528.
[88] The European Parliament [EP] & The Council of the European Union [EUCO] (2016) "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)." *Official Journal of the European Union*. P. 43-44

[89] EP and EUCO 2016, 31.

of privacy and personal data, where it is specifically targeted at stopping companies and organisations from taking advantage of and processing personal data. As it is wide and substantial in its form, just a few of the key articles will be highlighted in this section. Turning back to the processing of personal data, this specific issue is widely covered in the GDPR. Regarding processing, Article 5 informs us that there has to be "specified, explicit and legitimate purposes" when collecting personal data; they shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject"; include security of the personal data processed; and, concerning privacy, processing personal data shall be done in "a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are processed."[90] Regarding the specificity of what is meant by lawful, Article 6 explains that this is determined through either consent given by the data subject; to fulfil a contract in which the data subject is a part; instances, where processing is necessary to "protect the vital interests of the data subject or of another natural person"; and, it is "necessary for the performance of a task carried out in the public interest."[91]

Following the legal framework for how processing of personal data should be carried out, the articles 12-22 directly addresses the rights of the data subject. They first underline the importance of transparent information and communication from the data controller to the data subject, that is, the information shall be provided in a "concise, transparent, intelligible and easily accessible form."[92] Notably, Article 13 and 14 describe how data controllers must inform data subjects, when and how they have collected their data;[93] Article 17 describes the right to erasure ('right to be forgotten'), in which the "data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay";[94] Article 19 requires data controllers to notify any third party that they have shared personal data with to rectify or erase said data if on the behest of the data subject;[95] Article 21 specifies the areas in which the data subject have the right to object to the processing of their personal data, which includes for marketing purposes, and the data controller must be able to provide compelling evidence for the continuation of processing on legitimate grounds if they do not stop.[96] These articles particularly inform the individual of their rights in accessing, obtaining,

[90] EP and EUCO 2016, 35-36.
[91] EP and EUCO 2016, 36-37.
[92] EP and EUCO 2016, 39-40.
[93] EP and EUCO 2016, 40-41.
[94] EP and EUCO 2016, 43-44.
[95] EP and EUCO 2016, 45.
[96] EP and EUCO 2016, 45-46.

and regaining control over their personal data, which data controllers must abide by in their processing of personal data.

When concerning the global outreach of the GDPR, there are several articles within the framework that encapsulate the global influence of the GDPR. First, Article 3 refers to the territorial scope of the GDPR, by stating that the processing of personal data of EU citizens must abide by the GDPR framework, whether or not the data is being processed in the EU or outside of the EU;[97] Article 25 requires all companies and organisations, even if based outside to EU, to implement wide appropriate technical and organisational measures at the outset of processing personal data, and to "integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects";[98] Article 27 refers back to Article 3, in that it requires data controllers not established in the EU to designate a representative in the EU, so the EU can ensure that the GDPR is enforced correctly;[99] Article 44 establishes the general principle for transfers of personal data to a third country or international organisation may only be allowed if the controller ensures proper safeguards for the personal data and the data subject's rights are enforced;[100] according to Article 45, the European Commission gets to determine whether a third country or international organisation "ensure an adequate level of protection," if this is ensured, the circumstances surrounding the adequate level of protection will be checked regularly;[101] Article 48 allows transfers of personal data to a third country but these "may only be recognised or enforceable in any manner if based on an international agreement […] in force between the requesting third country and the Union or a Member state";[102] lastly, Article 50 emphasises and allows for the cooperation between the EU and a third country or international organisation in developing international cooperation on the protection of personal data, to "provide international mutual assistance in the enforcement of legislation for the protection of personal data," to promote cooperation by engaging the relevant stakeholders, and to "promote the exchange and documentation of personal data protection legislation and practice." [103] These articles demonstrate the GDPR's global outreach as they have direct influence on non-EU companies and organisations in forcing them to comply with the regulation if they wish to process personal

[97] EP and EUCO 2016, 33-34.
[98] EP and EUCO 2016, 48.
[99] EP and EUCO 2016, 48-49.
[100] EP and EUCO 2016, 60.
[101] EP and EUCO 2016, 61.
[102] EP and EUCO 2016, 64.
[103] EP and EUCO 2016, 65.

data of EU individuals. The regulation ensures EU individuals' right to having their personal data adequately protected along with their right to, in some degrees, removing consent to having their data processed, and controllers' and processors' responsibility to comply with all these provisions.

Digital Sovereignty for Europe

The changing digital technological reality is of high importance in the EU, so much so that the notion of 'digital sovereignty' has gained great importance on both a principal level but also on a structural level in a way that it is a pillar in instructing many digital technological policy initiatives. As according to the European Parliamentary Research Service (EPRS), digital sovereignty has "emerged as a means of promoting the notion of European leadership and strategic autonomy in the digital field."[104] They further state that the notion stems from a need to be able to meet the threat of non-EU companies on personal data protections of EU citizens, hence, it "refers to Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation."[105] Specifically, the European Council "has stressed that the EU needs to go further in developing a competitive, secure, inclusive and ethical digital economy with world-class connectivity," with a main highlight being AI and data security.[106]

Regarding privacy and data protection specifically, concerns are raised over the influence and power held by major technology companies, who collects and exploits "online users' data to generate advertising revenue" as part of their economic model.[107] This concern is combined with evidence that personal data collected via online platforms can be exploited for political reasoning, as shown by the Cambridge Analytica scandal.[108] While concerns of data exploitation is primarily based on U.S. companies – Google, Apple, Facebook, Amazon, and Microsoft (GAFAM) – concerns of cybersecurity has been raised on the grounds of Chinese 5G technology (as the U.S. have also raised concerns) and the possibility of foreign influence over a weak European cybersecurity.[109] Concern is also based on the EU's "lack of control over data produced on their territory," which applies to the fact that the "global public

[104] European Parliamentary Research Service (2020) "BRIEFING: Digital Sovereignty for Europe." *EPRS Ideas Paper* July 2020: 1-12. P. 1.
[105] Ibid.
[106] Ibid.
[107] European Parliamentary Research Service 2020, 3.
[108] Ibid.
[109] European Parliamentary Research Service 2020, 4.

cloud market is currently largely dominated by US and Asian companies."[110] Further, the GAFAM's control over data is problematised as being an issue for competitiveness in innovative markets, since their dominating presence mean that critical digital infrastructure could be dominated largely by non-EU companies.[111]

As illustrated by these concerns, many considerations fall into the EU's thinking in further developing frameworks for digital technological development. Here, digital sovereignty becomes a sort of umbrella term and goal at the same time, in that it is simultaneously informing policy and regulatory initiatives but also serves as an end-objective of the EU gaining more control over their critical digital infrastructure and in ensuring protection of privacy and personal data. Initiatives that have been implemented to address these concerns entail, for example, the GDPR as the overarching regulation to protect EU citizens from having their personal data exploited by third countries, companies, and organisations. Additionally, as immediately relevant, initiatives include the Cybersecurity Act, the Data Act, and the Data Governance Act (DGA) among other initiatives. The Cybersecurity Act has been implemented to tackle cybersecurity threats and attacks, as well as it "establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices."[112] The act is supposed to enhance citizens' trust in technology since their devices will be secure, be beneficial for businesses as the act entails a one cybersecurity certification, making it more efficient for businesses,[113] and lastly governments, who will also be better informed in their purchases of digital technological devices.[114] The DGA and the Data Act, initiated through the European strategy for data, should be understood as responses to foreign data control, specifically the U.S. CLOUD Act. These new acts – the DGA and the Data Act – are extensions to the EU data protection framework since the GDPR specifically aim to protect personal data, and the newer acts set out to protect nonpersonal data, hence, they "provide an additional framework the reuse, transfer, and protection of nonpersonal data."[115] The DGA sets out to strengthen sectors of the economy by "[facilitating] data sharing across sectors and EU countries, in order to leverage the potential of data for the benefit of EU citizens and

[110] Ibid.
[111] Ibid.
[112] European Commission (2018) "EU Negotiators Agree on Strengthening Europe's Cybersecurity." December 10, 2018. Accessed April 17, 2023 - https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6759
[113] Ibid.
[114] European Commission (2019) "Questions and Answers – EU Cybersecurity." June 26, 2019. Accessed April 17, 2023 - https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369
[115] Wood, Georgia and James Andrew Lewis (2023) "The CLOUD Act and Transatlantic Trust." *Center for Strategic and International Studies*, March 29, 2023. Accessed April 15, 2023 - https://www.csis.org/analysis/cloud-act-and-transatlantic-trust

businesses."[116] The Data Act tackles who can access and "create value from European data and where this can take place."[117] Thus, digital sovereignty and the initiatives being instructed under this notion are formed by a security concern over EU-dependence on non-EU companies in further constructing its critical digital technological infrastructure.

The U.S.-EU partnership and data governance

The U.S.-EU collaboration on developing guidelines to safeguard data flows and privacy are tightly connected to trade and their economic relationship, and a broader framework has been initiated and developed over the last several years to ensure the coexistence digital trade and privacy. One area of disagreement between the two have been the U.S. CLOUD Act. As a part of the CLOUD Act and the U.S.'s promotion of bilateral agreements has been initiated from the U.S.'s wish to be able to collect critical information from global communications providers, where data is stored in a different country and, hence, subject to different legal jurisdictions, a main worry for the EU has been the protection of EU citizens personal information. These worries stemmed from earlier experience of U.S. surveillance and misuse of data and so "the CLOUD Act faced criticism and concern from the EU officials worried that it would infringe upon European digital sovereignty."[118] Initial negotiations between the U.S. and the EU began in 2019 on how to facilitate transfer of critical information but stopped again quickly because of internal disagreements within the EU, but these disagreements have from the beginning of 2023 cleared up. Here, a consensus within the EU has been reached on "cross-border access to e-evidence with similar authorities as the CLOUD Act [which] signals real progress on reaching an e-evidence agreement between the European Union and the United States."[119] As pointed out by Wood and Lewis, a conflict will remain between implementing the CLOUD Act in accordance with EU regulations if the U.S. and the EU cannot settle on an agreement on e-evidence (critical information). So far, the challenges to aligning these are to be found within the GDPR framework of article 48, which states that an international agreement is necessary if a foreign court order should "be sufficient to make a transfer lawful."[120] Article 49 might be able to align EU regulation with the CLOUD Act, however, as it "establishes the conditions under which an international transfer could occur if an international agreement is not place,"

[116] Cyber Risk (na) "The European Data Governance Act (DGA)." Na. Accessed April 17, 2023 - https://www.european-data-governance-act.com/
[117] Wood and Lewis 2023 - https://www.csis.org/analysis/cloud-act-and-transatlantic-trust
[118] Wood and Lewis 2023 - https://www.csis.org/analysis/cloud-act-and-transatlantic-trust
[119] Ibid.
[120] Ibid.

which would be to notify the subject and receive consent or the transfer should be important for public security.[121] As already noted, collaboration between the U.S. and the EU on safeguarding data transfer and privacy has reached a new period, beginning with President Biden's signing off the Executive Order to Implement the European Union-U.S. Data Privacy Framework in October 2022, which was initiated in the beginning of 2022 to guide the legal framework for transatlantic data flows.[122] This has further been welcomed by the European Commission's draft adequacy decision which "concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to the US."[123] The legal framework was further acknowledged by the European Data Protection Board (EDPB) as having improvements from earlier U.S. legal frameworks but that it should be subject to frequent revision after reviews of the adequacy decision.[124]

China

China's data regulatory framework is not collected under one comprehensive national law but rather various laws and regulations addressing issues of personal data protection, data security, and cybersecurity. However, China has three main pillars constituting its data regulatory framework, these being the 2017 Cybersecurity Law (CSL), the 2021 Data Security Law (DSL), and the 2021 Personal Information Protection Law (PIPL), along with supporting administrative draft measures. Some scholars argue that China's framework can be compared to the EU's GDPR in constructing a more comprehensive data regulatory framework for themselves, but that the two frameworks still largely vary in content and their prioritisation of

[121] Ibid.
[122] The White House (2022) "FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework." *Biden White House*, October 7, 2022. Accessed April 16, 2023 - https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/
[123] European Commission (2022) "Questions and Answers: EU-U.S. Data Privacy Framework, draft adequacy decision." December 13, 2022. Accessed April 16, 2023 - https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632
[124] European Data Protection Board (2023) "EDPB Welcomes Improvements under the EU-U.S. Data Privacy Framework, but concerns remain." February 28, 2023. Accessed April 16, 2023 - https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en

privacy versus security.[125] This does, however, still speak to a level of comprehensiveness under which data regulatory frameworks are beginning to exist.

Similar to the EU, China, in the formation of a data regulatory framework, operates under a concept to form the foundation upon which laws and regulations are developed and implemented. Where the EU operates under the notion of 'digital sovereignty,' China has the notion of 'cyber sovereignty,' which is a notion emerging from a 2010 White Paper called The Internet in China. In the White Paper, 'internet sovereignty' which has later become 'cyber sovereignty' is described as deeply connected with network security. Specifically, the paper states that "within Chinese territory the internet is under the jurisdiction of Chinese sovereignty. The internet sovereignty of China should be respected and protected." [126] The 'cyber sovereignty' notion instructs domestic policy formation, while also instructing an approach to international diplomacy, in which sovereignty is a main pillar of state-to-state relations also applying to cyberspace. This is because the idea of cyber sovereignty promotes "that states should be permitted to govern and monitor their own cyberspace, controlling incoming and outgoing data flows," accordingly to how each state see fit.[127] The international dimension of 'cyber sovereignty' will be examined further together with how China is influencing global data governance, following first a presentation of how China has shaped its current framework for data legislation and regulations.

China's national data regulatory framework

Beginning this section is the introduction of the CSL, which was enacted in 2016 and came into effect in 2017, and its major importance for the further development of data laws and regulations in China. Following, articles from the CSL explaining its outreach and goal will be presented. From Article 1 of the CSL it is articulated that the law sets out to "safeguarding network security, safeguarding cyberspace sovereignty, national security, and public interests, protecting the legitimate rights and interests, legal persons, and other organizations."[128] Article

[125] Geller, Anja (2020) "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective." *GRUR International* 69 (12): 1191-1203. P. 1193.
[126] The Information Office of the State Council of the People's Republic of China (2010) "The Internet in China." *China Daily*, June 8, 2010. Accessed March 28, 2023 - https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm
[127] Parasol, Max (2018) "The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, and on China's Big Data and Smart City Dreams." *Computer Law and Security Review* vol. 34: 67-98. P. 81.
[128] Xinhua News Agency (2016) "Cyber Security Law of the People's Republic of China." *Cyberspace Administration of China*, November 7, 2016. Accessed March 27, 2023 - http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

21 starts with introducing measures to ensure network security through "a network security graded protection system" implemented by the state.[129] This article refers to the responsibilities of network operators to "protect the network from interference, destruction or unauthorized access, and prevent network data from being leaked or stolen or tampered with."[130] In general, Article 21-28 all function as legal guidelines to network operators by instructing how they should further ensure network security.

Article 37 of the CSL is one of the more significant ones of the framework, since Article 37 establishes strict localisation rules of network operators in China. Specifically, it is operators of critical information infrastructure that must abide by the rule of localising the personal data and important data that they collect in China, meaning whatever data they have collected in China must also be stored in China. The article further explains the structure around this process regarding transfer of data, that if it is necessary to fulfil the needs of a specific company then a "security assessment shall be conducted in accordance with the measures formulated by the national network information department in conjunction with the relevant departments of the State Council."[131] This article becomes significant in its formulation and implications. First, what classifies as 'important data' is rather undefined. Second, strict localisation rules can prove to have costly implications for both foreign enterprises, who will have to establish and run domestic servers in China for the data collected, as well as domestic companies who fear "that this rule may hinder their global operations and expansion."[132] As argued by Geller, "strict data localisation is seen as an important means to achieve cyberspace sovereignty and network security, the main goal of the CSL. Beyond that, it is supposed to strengthen supervision and legal enforcement."[133] Articles 40 and 41 establishes the foundations for how operators should handle personal data collected. Article 40 instructs that user information collected shall remain confidential and that network operators shall "establish and improve user information protection systems."[134] The seriousness of this is further emphasised in Article 41, which requires that "network operators shall follow the principles of legality, legitimacy, and necessity, disclose rules of collection and use, expressly state the purpose, method and scope collection and use of information, and obtain the consent of the person [having their data]

[129] Ibid.
[130] Ibid.
[131] Ibid.
[132] Geller 2020, 1200.
[133] Ibid.
[134] Xinhua News Agency 2016 - http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

collected."[135] It should be emphasised that the CSL is largely concerned with establishing proper structures that will advance the security of cyberspace, and therefore gives less attention to personal data protection. In this regard, the CSL differs in its main priority from the EU's GDPR. Hence, the specific, recurring focus on networks and network operators is relevant to understand the CSL's main priority of cyberspace security.

Where the CSL focuses on networks and network operators, the DSL, put into effect in 2021, is based around forming a legislative framework for processing data, securing data, as well as "promoting development and utilization of data, protecting the lawful rights and interests of individuals and organizations, and safeguarding the sovereignty, security, and development interests of the state," as per Article 1 of the DSL.[136] Article 31 of the DSL confirms the authority of the CSL by establishing that the provisions of the CSL shall apply to cross-border data transfers for data collected and processed in China. It further explains that the specific measures for managing outbound security of what it calls important data from critical information infrastructure operators "shall be formulated by the national cyberspace authority in conjunction with the relevant departments under the State Council."[137] By important data, this article refers to Article 21 of same law, the DSL, in which it is referred to as "data concerning national security, lifelines of the national economy, important aspects of people's lives, major public interests, etc., are core data for the state, for which a stricter management system shall be implemented."[138] Likewise, Article 36 of the DSL instructs aspects of cross-border data transfers, but in this instance if data is being requested transferred out of China by another country's judicial or law enforcement authority. The article stipulates that a request like this will be handled by the competent authorities of China, in estimating whether a transfer is legitimate "is accordance with the relevant laws and international treaties or agreements concluded or acceded to by the People's Republic of China, or in accordance with the principles of equality and reciprocity."[139]

The PIPL, which was put into effect in 2021, was initiated as part of the 2018-2023 National People's Congress Standing Committee Five-year Legislative Plan. The need for this was explained by Zhang Yesui, spokesman for the second session of the National People's

[135] Ibid.
[136] The National People's Congress of the People's Republic of China (2021) "Data Security Law of the People's Republic of China." *NPC*, June 10, 2021. Accessed March 21 2023 - http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml
[137] Ibid.
[138] Ibid.
[139] Ibid.

Congress, as being necessary to provide one legislative plan, since regulations on personal information protection had so far been scattered around a variety of different laws. Zhang explained, "we need to have a law specifically on the protection of personal information to form a unified force of regulation."[140] As set out in Article 1 of the PIPL's general provisions, the law is enacted to "protect the rights and interests of personal information, regulate personal information processing activities, and promote the rational use of personal information."[141] Article 3 of the PIPL addresses the extraterritorial dimension of processing personal information in the law – processing is to occur within the territory of the People's Republic of China, except for three specific circumstances, where processing of data collected in China can occur outside of China's territory: "(1) For the purpose of providing products or services to domestic natural persons; (2) Analysing and evaluating the behaviour of domestic natural persons; (3) Other circumstances stipulated by laws and administrative regulations." [142] Additionally, the law establishes a framework for personal information protection regarding consent, management of consent, and rules of personal information processing. Regarding the latter, the PIPL is rather comprehensive in its format, establishing Article 13-37 all regarding rules of processing personal information, the user's right of consent, when to collect consent from parents in case of a minor, and specific rules for how personal information processors must handle the data they collect. Lastly, a relevant an interesting part of the law is the section on cross-border data transfer. Firstly, for a personal information processor to transfer data outside of China's territory, it must be for business or other specific needs, there needs to be a reason for the transfer, as according to Article 38.[143] Article 40 establishes that to transfer the data out of China's territory "it shall pass a security assessment organised by the national cyberspace administration."[144] Article 41 of the PIPL aligns with Article 36 of the DSL by further establishing that should a foreign judicial or law enforcement agency request to have personal information transferred, this will also be on the behest of the competent authorities in China to decide "in accordance with relevant laws and international treaties and agreements concluded or acceded to by the People's Republic of China, or in accordance with the principle

[140] Zhao, Xinying (2019) "Legislation Coming to Better Protect Personal Details, Spokesman Says." *China Daily*, March 4, 2019. Accessed March 22, 2023 - https://www.chinadaily.com.cn/a/201903/04/WS5c7cbaa4a3106c65c34ec9ae.html
[141] The National People's Congress of the People's Republic of China (2021) "Personal Information Protection Law of the People's Republic of China." *NPC*, August 20, 2021. Accessed March 21, 2023 - http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[142] Ibid.
[143] Ibid.
[144] Ibid.

of equality and reciprocity."[145] In regard to cross-border transfers, the law continues with Article 42 establishing consequences of infringing on natural people's personal information protection rights in China. Article 42 exclaims that if foreign organisations or individual infringe on said rights "or endanger the national security and public interests" of China, then they might consequentially be prohibited from or have restricted access from personal information.[146]

China's data regulatory framework illustrates the country's increased need for control over the collection, storage, and use of data within its borders, as a means of heightening national security. The three main pillars of China's regulatory framework target data and privacy protection, and an increased security of cyberspace, which are all ultimately affecting the activities of foreign companies and organisations in China. Hence, these laws also create an environment for Chinese domestic companies to have greater influence on China's national digital technological development.

China's influence on global data governance

In examining China's influence on global data governance there are various initiatives of relevance. First is China's efforts to influence international standard setting through international institutions, such as through the United Nations agency the International Telecommunications Union (ITU), the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC), and the 3rd Generation Partnership Project (3GPP), hence, active in setting and forming standards and procedures regarding digital technologies.[147]

Second initiative of relevance is the Digital Silk Road (DSR), which was launched in 2015. The DSR is formally a part of the bigger Belt and Road Initiative (BRI), China's international investment and infrastructure initiative. Where the BRI aims to improve global physical connectivity, the DSR aims to improve global digital connectivity. The specifics of the initiative is more complex, as what counts as official DSR projects is not always clear, as well as with the actors participating, meaning it is not always clear whether a project or trade being

[145] Ibid.
[146] Ibid.
[147] Paszak, Pawel (2020) "China's Growing Influence in International Organizations." Warzaw Institute, October 14, 2020. Accessed April 2, 2023 - https://warsawinstitute.org/chinas-growing-influence-international-organizations/

undergone by a Chinese tech company in a foreign country is a part of the DSR or not. As explained by Ghiasy and Krishnamurthy, there is a macro and micro level to the DSR: the macro level "is about the development and interoperability of critical digital infrastructure such as terrestrial and submarine data cables, 5G cellular networks, data storage centers, and global satellite navigation systems"; the micro level refers to "[promoting] connectivity between local businesses and consumers."[148] Chinese tech companies being internationally active is not new with the DSR, they have been operating and expanding their operations globally for decades. Rather, the DSR can be understood as a sort of broader structure, wherein Chinese digital infrastructure projects are collected under the umbrella of the DSR – even if some of these projects are not affiliated with the Chinese state or receiving financial support from the state. However, as argued by Greene and Triolo, "projects self-brand as part of the DSR to score political – and perhaps financial – support from Beijing, while the state, is not too involved in day-to-day operations, although it can and does intervene to advance its strategic objectives."[149] As further emphasised, "some projects are, however, highly state-influenced."[150]

The geopolitical context in which the DSR operates is becoming highly complicated because of various issues. This is particularly by U.S. and EU worry over Chinese state influence on Chinese tech companies in their international operations. Several Chinese tech companies, like Huawei and TikTok owned by ByteDance, have been increasingly securitised by the West over several years together with how U.S.-China relations have worsened, which is most likely "increasing the likelihood that Washington and EU countries will intensify efforts to constrain China's technological influence."[151] The worries expressed by the West in this instance might not be completely unfounded, since China through its expansion of the DSR and the BRI is actively promoting "to fully respect cyber sovereignty"[152] with member countries of the DSR, which stands in contrast to a more liberal, market-oriented friendly approach of promoting a free internet and the free flow of data being done by the West, the

[148] Ghiasy, Richard and Rajeshwari Krishnamurthy (2021) "China's Digital Silk Road and the Global Digital Order." *The Diplomat*, April 13, 2021. Accessed April 1, 2023 - https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/

[149] Greene, Robert and Paul Triolo (2020) "Will China Control the Global Internet Via its Digital Silk Road?" *Carnegie Endowment for International Peace,* May 8, 2020. Accessed April 1, 2023 - https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

[150] Ibid.

[151] Ibid.

[152] Internet Communication Magazine (2018) "'One Belt, One Road' Digital Economy International Cooperation Initiative Released." *Cyberspace Administration of China*, May 11, 2018. Accessed April 2, 2023 - http://www.cac.gov.cn/2018-05/11/c_1122775756.htm

U.S. in particular. However, while this conflict continues, along with worries of data protection, it is less relevant in countries outside of the West which are already a part of the DSR and BRI, such as countries in Africa and Central Asia.[153] Hence, the DSR and Chinese tech companies' gradual expansion of their global operations, together with Chinese state involvement in some aspects and Western worry of surveillance, leading to securitisation of Chinese digital technologies "will likely cause dramatic and perhaps irreversible shifts in cyberspace governance and telecommunications standard-setting."[154]

Summary

The three cases illustrate the shift in data governance, which has occurred in the last decade, and the various approaches that states can choose in forming their different regulatory frameworks. The shift illustrates a move away from the U.S. dominated data governance with major actors in the digital economy, like the EU and China, forming their own regulatory frameworks from their own priorities concerning privacy and data protection. The U.S. approach of data governance led to the domination of major tech companies in control of data. The EU approach of implementing the GDPR has forced foreign tech companies to adjust to EU standard, triggering the Brussels effect, where "GDPR's data transfer rules are increasingly forcing the adoption of similar approaches elsewhere as a condition of digital access."[155] Likewise, China has also triggered the Beijing effect of influencing global data governance, as through the DSR, where Chinese technologies and approaches of state-centralised data governance hold influence.[156] The three actors showcase how the unregulated control of data has led to a global fragmented data regulatory framework, in which states form their own frameworks based on different priorities – market oriented, privacy protection, national security – resulting in data and the influence on data governance becoming an area of increased competition for global influence.

[153] Ibid.
[154] Ibid.
[155] Arner et al. 2022, 663.
[156] Ibid.

Theoretical assessment

As a non-physical asset, data is extremely difficult to control, which has only become harder with decades of either non-existing regulatory framework or loose regulatory framework, mostly consisting of principles rather than actual legislation. The implementation of vastly different approaches to data governance by three major actors in the digital economy illustrates a tentative shift in the assumption of digital data's relevance and importance by data becoming increasingly more controlled to benefit the interests of each state. In this part, the thesis will examine theoretical approaches to the current shift in global data governance, as to why states are having a heightened focus on controlling data, and the limits and possibilities of controlling data, and how the topic can be assessed within IR theoretical frameworks. Specific focus within the latter part will be given to the question of whether data and the movement of data constitutes a size of great relevance that affect states interests and motivation for power – or vice versa, if power rivalry is what constitutes the shift in data governance – or if data merely should be considered a secondary factor to how states shape their interests.

Forming a theoretical foundation for the shift in data governance

As laid out in the above, the three actors have different reasons for designing their data regulatory frameworks as they have done – the U.S. advocates for the free flow of data with limited regulations to favour their domestic tech industry, while also showing protectionist tendencies by sanctioning specific foreign companies; the EU has created a framework on the basis of data and privacy protection, while adopting the notion of 'digital sovereignty' to instruct further policy action in the direction of protecting EU territory and promoting EU companies in further development of critical digital technological infrastructure; China has created a framework under the notion of 'cyber sovereignty,' which entails strict localisation laws to ensure security of cyberspace and data, which also has protectionist tendencies, by limiting foreign companies' activities in China and instead promoting domestic tech companies. As already explained, the U.S. and U.S. based tech companies have been dominating in global data governance thus far, therefore the interesting outliers in this equation is the EU and China in designing their data regulatory frameworks. Several events have revealed the vulnerability, and therefore importance, of data concerning politics, such as the Snowden revelations of extensive surveillance by American intelligence. Additionally, the Cambridge Analytica scandal, where data from millions of U.S. Facebook users were harvested unauthorised for

political campaigning caused concerns for data protections. While efforts to regulate cyberspace and data in these frameworks are not new, the extensive reach that they are forming are, resulting in a new level of geopolitical and economic competition for data governance.

Of the theories presented in the above theoretical section of the thesis, two theoretical frameworks can help explain the reasoning behind the heightened focus on data regulation. Of these, the theoretical understanding of deterritorialisation can highlight the effect of data going unregulated as it has. Deterritorialisation in connection with data should be understood as phenomenon deriving from the global internet and a deterritorialisation of cyberspace, resulting in a rapid merge of cultures and social relations. This results in a structure of a non-physical thing, data via the internet, challenging and moving already set territories of nation states with physical borders. Alas, the rapid development of digital technology in the form of the internet and digital platforms have resulted in a breaking down of traditional territorial and cultural boundaries, instead creating a space where social relations are being altered and organised through communication networks. Because of this, cultural, social, and political relations participate in new economic and social activities, which extends itself beyond the physical territories. It is within this deterritorialised space that data have been able to roam relatively freely. Second phenomenon that is useful in understanding the shift in data governance is surveillance capitalism, which occurs as an extension of the deterritorialisation of the internet and data. Through this scope, data is the essential factor in tech corporations' business structure, wherein data is extracted from their users, processed, and sold off. Through this lens, tech corporations gain financial means, become more powerful as dominating actors in the digital technological sphere, and are able to use said data for further innovation and development of their businesses. As according to Zuboff's argument, this leads to behavioural modification of its users, since the tech corporations exploiting our data holds power and influence because of it, triggering change in our behaviours by predicting and deciding on our needs. The growing influence and power that tech corporations hold, Zuboff terms instrumentarian power as they are now able to automate its users – the use of digital platforms in exchange of one's data is no longer just a form of transaction, it is instead forced submission and an accept to modify one's behaviour.

From this foundation, data has moved freely through a deterritorialised space, which has left data to be exploited by corporations as powerful actors and challenged the territories of nation states. This can especially be seen from the actions of the EU and China in the formation of their different but comprehensive data regulatory frameworks. Specifically, the notions of 'digital sovereignty' and 'cyber sovereignty,' which each actor has adopted as

principles guiding their policy and regulative initiatives regarding digital technological development, informs of a reaction to the deterritorialisation of data. The deterritorialisation of data, its transcendence beyond physical borders, and its further exploitation by private corporations can from a state sovereignty point of view be regarded as a problem, or even threat, to the sovereign state. Hence, these notions of digital or cyber sovereignty functions as discursive tools, which legitimise the actions of the state in its efforts to (re-)centralise control of data and data flows. This creates a process of reterritorialisation, where the practices of the state "can be read as elements of geopolitical visions that problematise specific threats, articulate specific images of an enemy, and, not least, (re)produce spatialities."[157] Returning to the various issues of a global fragmented data regulatory framework, approaches to reterritorialisation through practices of digital and cyber sovereignty are contradictory to and "in tension with processes of global interconnectedness." [158] Thus, through the lens of sovereignty and traditional territory, the free flow of data across borders are challenging states, and therefore they decide to act by e.g., legislative and regulative action, in (re)producing territory based on a "normative assumption that all online activity that occurs 'in' a country (because user, servers, or data are 'located' there) should be treated as a part of a corresponding cyberspace territory."[159] Referring back to the dominance of powerful private corporations in the surveillance capitalism framework, these corporations are also actors participating in the reterritorialisation process in what Lambach coins 'ecosystems,' which "are based on the integration of multiple services, creating a denser network at their core, while their borders remain relatively porous."[160] These companies create new virtual territories that is either enduring enough for user to want to be in or a necessity to pass through, and design these virtual territories through the use of "digital rights management software, limited licenses, cookies, and signup requirements to create boundaries that allow for data collection, user surveillance, and the monetization of access to digital content."[161] These practices reterritorializes by drawing new boundaries, "which create lock-in effects, thus hardening the borders between ecosystems."[162] It is precisely this reterritorialisation being done by private companies through their boundary drawing practices of territorialising via their digital platforms, while exploiting

[157] Glasze, Georg et at (2022) "Contested Spatialities of Digital Sovereignty." *Geopolitics* 28 (2): 919-958. P. 921.
[158] Ibid.
[159] Lambach 2020, 494.
[160] Lambach 2020, 498.
[161] Ibid.
[162] Ibid.

data of its users, that states are responding to. By performing their own reterritorial practices through claiming digital and cyber sovereignty and implementing policies and laws to support their sovereignty, "geopolitical confrontations intersect with geoeconomics competition in a complex way."[163]

Governing data on the local and global level

Following these actions of reterritorialisation in facing deterritorialisation and surveillance capitalism, and with this leading to a shift in data governance (which is in general combined with increased competition in technological innovation and R&D), it can be argued that states are moving in a techno-nationalist oriented direction, while also operating within neo-techno-nationalist frameworks, when concerning the global level. As laid out by the case study analysis, the U.S., the EU, and China, despite their different approaches to regulating data control and data flows, all have in common a discursive approach by justifying their motivations as based on issues of national security. These concerns of security are formed around the concerns of the nation state, or in the case of the EU, the security of the bloc. The three actors are in this regard through various strategies, laws, and discourses, creating a foundation of national or bloc interests, which shall instruct the further development of their technological capabilities and industries and links these directly to the "national security, economic prosperity and social stability" of their nations.[164]

In the case of China, its data regulatory frameworks are comprehensive in its centralisation of data and data security, with strict localisation laws making it more difficult for foreign companies to operate in China, as well as promotion of domestic industries, its approach could be concluded to solely being one of a techno-nationalist framework. However, China's process of implementing its regulatory framework does not only hold concern for the local level, but it also holds space for the global structure. The actual process of writing and implementing the laws examined in the case study is evidence of this two-fold interrelation, in which laws are written with subsequent draft measures published followingly. This process allows for companies and other organisations, foreign and domestic, to respond the initial legislative proposal and negotiate the further regulatory developments.[165] Although this process leaves room for negotiation and opportunity for influencing further regulatory

[163] Glasze et al. 2022, 923.
[164] Capri, Alex (2020) "Techno-Nationalism and Diplomacy: the US-China Race to Reshape Alliances, Institutions and Standards." *Hinrich Foundation* October 2020: 1-44. P. 4.
[165] Parasol 2018, 68.

developments, the implementation of the laws are still quite protectionist in their nature, as the restrictions of cross-border data flows ultimately stems from national interest of security and promotion of national industries in building critical digital technological infrastructure. Likewise, as China, the EU's data regulatory framework and adoption of digital sovereignty implies a move in the direction of techno-nationalism. Whilst the GDPR is less strict than China's laws regarding localisation, the GDPR is still thorough and comprehensive in its formulation of users' rights concerning their private data, forcing companies to comply if they wish to operate in the EU. Simultaneously, the EU data regulatory framework does not deny the reality of global digital connectivity and does not try to prevent it completely, it is however, focused on centring European industries in its further digital development. Lastly, the U.S. could seem contradictory in this setting, having dominated global data governance for so long with a principle of free flow of data, and still advocating this principle. The heavy emphasis on free flow of data while governing data on a foundation of globalisation and free market ideology would indicate a techno-globalist framework. However, the actions of the U.S. in the increased digital development competition of export and import controls, sanctions, and discursive and diplomatic frameworks for securitising specific foreign tech companies – here among predominantly Chinese tech companies – are protectionist actions to secure the continued dominance of U.S. tech companies. This, coupled together with diplomatic work to advance their stance on data regulation with like-minded states, indicates that the U.S. as well is moving in a direction of techno-nationalism, where its political incentives are being developed around concerns of the nation state and national security.

A distinctive element of the three actors' frameworks is how these states also operate through techno-diplomacy, in trying to protect their nationalist technological interests. Techno-diplomacy being a conceptualisation of "advancing a nation's techno-nationalist agenda through enticements, partnerships, and concessions, as well as through the threat of negative outcomes."[166] One example already examined in the case study analysis is the U.S.-EU developing partnership on cross-border data flows, however, several more of this kind exists. Further examples of this practice are China's Global Initiative on Data Security and the U.S.'s Clean Network Program. The Clean Network Program directly "seeks to expunge Chinese technology from carrier networks, data storage, mobile apps, cloud networks and undersea cables" in partnership with other countries by abiding in specific principles of how to approach

[166] Capri 2020, 4-5.

and what to allow regarding sharing of technology and data protection.[167] In the Global Initiative on Data Security, China advocates for global cooperation on securing data and "call on all states to put equal emphasis on development and security, and take a balanced approach to technological progress, economic development and protection of national security and public interests."[168] It can be argued that the Chinese initiative is a response to the U.S. Clean Network Program. Regardless, as techno-diplomacy stems from a concern of national needs and interests, "policy makers increasingly look to draw upon common values and leverage each other's markets, resources, and firms."[169]

To summarise, the EU and China are two actors that have been showing distinctive signs of increased techno-nationalist tendencies within the last decade, which are distinctive because of their notions of digital and cyber sovereignty. However, the U.S. is showing just as techno-nationalist tendencies in its protectionist policies and promotion of domestic industries, it is rather that the U.S. has not needed to conceptualise a framework for sovereignty as they have been positioned as global hegemon for so long, extending to its technological dominance. Ultimately, the EU and China's move to a more techno-nationalist orientation can be understood as a reaction to U.S. dominance of digital development, and their notions of digital and cyber sovereignty as a way of (re)gaining control in this domain. The neo-techno-nationalist orientation of the frameworks stems from an acknowledgement that the global level of the digital structure cannot be ignored, and that the states will have to interact with it. However, the motivations behind interaction with the global level are primarily shaped by techno-nationalist sentiments, in that the states interact with the global level because of concerns of national security and gaining influence and control of their own digital territories.

Realist and constructivist perspectives on the fragmented data regulatory framework

Having established a theoretical foundation upon which the global fragmented data regulatory framework has been developed, and determined that this is a part of a greater occurrence of techno-nationalism, this section of the theoretical assessment will analyse data and data governance and its influence on international political change from a realist and constructivist

[167] Capri 2020, 4.
[168] Ministry of Foreign Affairs of the People's Republic of China (2020) "Global Initiative on Data Security." *MFA of the PRC*, September 8, 2020. Accessed April 20, 2023 - https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html
[169] Capri 2020, 5.

perspective. The foundation of the fragmented framework consists of states, with reasons of deterritorialisation and surveillance capitalism, having developed more strict and controlled data governance frameworks, i.e., creating processes of reterritorialisation in attempts to support their traditional physical boundaries of sovereign territories.

As explained in the theory section of this thesis, these two theoretical frameworks have very different approaches to the relationship between technology and international political change. However, both theoretical frameworks are primarily of the conviction that technology is a secondary factor in the formation of international relations and evaluations of power and "tend to treat technology as external to politics, not as something integral to how contemporary politics and world affairs are carried out."[170] A relevant point of departure in assessing the data regulatory frameworks presented, is from the practices unfolding from the discursive guise of national security, from which a realist and constructivist perspective are different. From a realist framework, the discursive approaches of national security from which practices unfolds in the form of protectionist policies and regulatory frameworks, relates itself to a general understanding of nation states as primary actors within an anarchic structure, and states needs to protect themselves. Following a realist framework in assessing states' individual control of data and global data governance, it can be argued that global data governance is a complex area to agree on regarding *how* it should be governed, since the distribution of power in the international system and how states utilise power, challenges a common approach of data governance. Data, in this sense, can be understood more as material capacity of a state, and the actors' approaches of (re)gaining control of data can be understood as ways of sharpening and defending territories. In this sense, the actions of reterritorialising are signs of national security concerns as other states' utilisation of power is threatening. Following a realist framework, data is still regarded as a secondary factor to international political change and its primary factors of security and material power. Data as technology does not hold the relevant influence to challenge the nature of international politics and relations, as "technology may change, and technology may also impact on international relations, but the nature of politics remains essentially the same."[171] By a realist perspective, data and frameworks of data governance are merely factors that can support superiority in certain aspects, such as (re)gaining sovereignty by (re)claiming a digital territory. Following a constructivist framework, it is less the functionality of a given technology that decides its relevance to international politics or actors'

[170] Eriksson and Newlove-Eriksson 2021, 5.
[171] Eriksson and Newlove-Eriksson 2021, 7.

perception of said technology. Rather, a given technology gains specific perceptions based on states' "identities, ideas and processes of socialization [more] than by technological development in and of itself."[172] It is based on this that states calculate levels of value, opportunity, and threat to a given technology. Considering the context of increased digital competition that the three actors are developing their data regulatory frameworks in, and in which the three actors are in rather complicated processes of socialisation, the actors are projecting a sense of vulnerability to data. The three actors are in different ways in conflict with one another over data flows and processing; the U.S. wants to retain its position of technological dominance and are reacting to China's increased influence as a powerful state by transferring a projection of threat to Chinese companies – they are, however, not responding harshly to the EU's regulatory framework, as these two actors through a long process of socialisation have established that they are similar in their values, and the U.S. is therefore instead proposing increased partnership on data; the EU has implemented laws controlling data and privacy security and continues to develop its framework, as a response to data exploitation by the U.S. and American companies; China is also controlling data and privacy security by a set of laws, here among localisation control, as well as a sense of threat of exploitation of data by foreign companies. All these approaches are unfolding under a discursive practice of claiming that action is necessary because of national security. Thus, by projecting ideas of threat onto data flows because of complicated processes of socialisation, the actors are able to legitimise their various measure of data control and limits by claiming national security.

Following the constructivist framework, the extraterritorial influence of the data regulatory frameworks in connection with other initiatives of the case study actors, can be regarded as vessels of norm diffusion. Individually, these take different forms: the U.S.'s position of dominance on global governance has included its tech industry, with U.S. companies dominating global digital technological development, as well as U.S. dominance of advocating free flow of data; the EU holds extraterritorial influence via its regulatory framework, through what is coined the Brussels effect, in which the EU's data and privacy norms gain international influence, as foreign companies advocate for similar implementations in other countries; and China, through norm-promoting initiatives like the DSR, where the ideal of cyber sovereignty is guiding in its implementation and development of DSR projects, hence, a norm diffusion of the ideal of how "states should have control over the digital technologies,

[172] Eriksson and Newlove-Eriksson 2021, 12.

content, and infrastructures within their jurisdictions."[173] As global data governance has been largely dominated by the West, and in particular the U.S., results of norm-promotion of Western cyber values and norms have been clearer for a longer while, "which is characterised by commitment to multi-stakeholderism and fundamental values, including the free flow of information, human rights and democracy." [174] However, the EU's adoption of digital sovereignty, design of a comprehensive data regulatory framework, and discussion of wider engagement and promotion of EU digital technological companies, is signalling the EU's "increasing influence […] as a distinctive cyber power [which] has called into question the U.S. dominance in cyberspace within the Western bloc."[175] Regarding China's norm-promotion through the DSR, it appears to have an attractive effect with several countries adopting principles from China's cyber sovereignty concept, e.g., from the 53rd Annual Session of the Asian-African Legal Consultative Organisation in 2014, where "the organisation established a working group to discuss state sovereignty and international cooperation in cyberspace."[176] With China being the one of the three actors with the most strict localisation and data security laws, it is especially interesting to consider China's efforts at norm-promoting its ideals of cyber sovereignty. Cyber sovereignty is a particularly difficult thing to obtain because cyberspace ultimately is difficult to control and limit as it expands beyond borders. However, by offering norms of cyber sovereignty, China is challenging U.S. dominance on global data governance, and offering other countries interested a way to also challenge the U.S., while also offering these countries digital products and services.[177] If China is successful in its norm-promotion by proving that it is possible to draw borders in cyberspace, i.e., reterritorialising through strict boundary-drawing, China will ultimately hold a much greater influence on global data governance than currently, and by that provide a regulatory framework for other countries to adopt as a contester to a predominately U.S.-led global data governance.

As realism and constructivism does provide ways of understanding technology's influence on international political change, and in this regard data's influence, these understandings are still relatively limited in their treatment of the actors involved and the changing nature of digital

[173] Liu, Lizhi (2021) "The Rise of Data Politics: Digital China and the World." *Studies in Comparative International Development* vol. 56: 45-67. P. 52.
[174] Gao, Xinchuchu (2022) "An Attractive Model? China's Approach to Cyber Governance and Its Implications for the Western Model." *The International Spectator* 57 (3): 15-30. P. 17.
[175] Ibid.
[176] Gao 2022, 24.
[177] Gao 2022, 26.

technology. First relevant aspect of mentioning in this regard, is realism's approach of solely acknowledging states as the primary actors and subjects of analysis. As illustrated throughout this analysis, the involvement and actions of non-state actors is of great importance in digital development and creation of data regulatory frameworks. Here among private tech companies, which have become a powerful force with political influence, as well as activists and whistle blowers, whose active campaigning also hold great influence in the development of data regulatory frameworks. Further, realism's relatively neutral understanding of technology does not necessarily help explain the probably more dynamic complexity of which rapid digital development involved. This stance tends to treat technology's relevance according to its functionality, i.e., 'good' if it does what it is supposed to, 'bad' if it does not,[178] and does not approach the 'good/bad' contradiction from a moral standpoint, which would help in the analysis of the relationship between technology's (here, data) and international political change, in understanding technology's influence on power. Likewise, constructivism's approach of viewing technology as an object upon which states project and perceive identities and norms, primarily limits itself in not considering how e.g., digital development challenges processes of socialisation. In this sense, constructivism fails to capture the complexity of how data, as a necessity for digital development, becomes an asset of its own right that exists on a larger plan than just as part of a development upon which states project identities and modify relations.

Conclusion

The case study analysis of the data regulatory frameworks of the U.S., the EU, and China have provided a necessary context for understanding the occurrence of the fragmented data regulatory framework, from which achieving an even global data governance is complex. This fragmentation in global data governance should be understood in the wider context of global power rivalry, where great powers are attempting to advance their interest domestically and abroad. Here, their different approaches of extraterritorial influence provide an example of how states are trying to influence international standard setting through normative settings, such as the distinction between 'digital sovereignty' and 'cyber sovereignty,' as well as ideals of free-flow of data and state-centred control of data. Who wins the fight for data governance – or 'who is right' – is the one who provides a framework that is both consistent in its form, efficient in its efforts, and provides a value-oriented legitimisation to its framework. Legitimising one's

[178] Carr 2016, 32.

framework starts by proving its domestic effect but is inherently fully legitimised through its extraterritorial reach when other states choose to adopt it. As a larger extraterritorial reach and influence both legitimises the domestic framework of regulatory and economic interests, it also becomes a vessel for norm diffusion adding to a position of leadership and increased power. From this, it can be determined that states have different interests in how they design and implement their data regulatory frameworks – with both domestic need and international influence in mind – but that essentially how they market their framework is equally as important. An attractive regulatory framework targeted correctly can help states gain influence internationally as standard setter, as the issue of global data governance is of great importance.

As this thesis has paid attention to how realism and constructivism, as dominating IR theoretical frameworks, treat technology, and thus, how they treat data's relevance to international political change, it can be argued that these theoretical frameworks are limited in their understanding of technology. As the rapid transformation that digital infrastructure has brought with it is complex and dynamic, ranging from issues of information-flow, connectivity, security, and economic development, data and new technological development should be considered as such: complex and dynamic. Hence, perspectives of realism and constructivism have their shortcomings in this aspect, as they tend to treat technology as a secondary factor to power and the formation of relations, when digital technology essentially has become the gateway for further global development. In approaching this topic further, it would be beneficial to first, include a wider IR theoretical framework to gain additional perspectives on the relationship between technology and international political change, in this case the influence of data on international politics. Further, a more extensive approach of combining IR theory with other theoretical paradigms, which takes the dynamic nature of technology more seriously, would be essential in incorporating better analysis of technological development into IR theoretical thinking.

Bibliography

Appadurai, Arjun (1990) "Disjuncture and Difference in the Global Cultural Economy." *Theory, Culture & Society* vol. 7: 295-310.

Arner, Douglas et al (2022) "The Transnational Data Governance Problem." *Berkeley Technology Law Journal* vol. 37: 625-700.

BBC (2020) "US Challenges 'Unfair' Tech Taxes in the UK and EU." *BBC News*, June 2, 2020. Accessed April 10, 2023 - https://www.bbc.com/news/business-52896266

Capri, Alex (2020) "Techno-Nationalism and Diplomacy: the US-China Race to Reshape Alliances, Institutions and Standards." *Hinrich Foundation* October 2020: 1-44.

Carr, Madeleine (2016) *US Power and the Internet in International Relations: The Irony of the Information Age.* Basingstoke: Palgrave Macmillan.

Castells, Manuel (2010 [1996]) "*The Rise of the Network Society*." Second Edition. Chichester: Blackwell.

Checkel, Jeffrey T. (1998) "Review: The Constructivist Turn in International Relations Theory." *World Politics* 50 (2): 324-248.

Cyber Risk (na) "The European Data Governance Act (DGA)." Na. Accessed April 17, 2023 - https://www.european-data-governance-act.com/

Data Protection Laws of the World (2023) "United States: Collection and Processing." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?c2=&c=US&t=collection-and-processing

Data Protection Laws of the World (2023) "United States: Law." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?c2=&c=US&t=law

Data Protection Laws of the World (2023) "United States: Security." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?t=security&c=US

Data Protection Laws of the World (2023) "United States: Transfer." *DLA Piper*, January 29, 2023. Accessed April 15, 2023 - https://www.dlapiperdataprotection.com/index.html?t=transfer&c=US

Dunne, Tim and Brian C. Schmidt (2014) "Realism." In The Globalization of World Politics: An Introduction to International Relations, Sixth Edition, 99-112, ed. by John Baylis, Steve Smith and Patricia Owens. Oxford: Oxford University.

Edgerton, David (2007) "The Contradictions of Techno-Nationalism and Techno-Globalism: A Historical Perspective." *New Global Studies* 1 (1): 1-32.

Eriksson, Johan and Lindy M. Newlove-Eriksson (2021) "Theorizing Technology and International Relations: Prevailing Perspectives and New Horizons." In *Technology and*

International Relations: The New Frontier in Global Power 3-22, ed. Giampiero Giacomello, Fransesco N. Moro and Marco Valigi. Cheltenham: Edward Elgar Publishing.

European Commission (2018) "EU Negotiators Agree on Strengthening Europe's Cybersecurity." December 10, 2018. Accessed April 17, 2023 - https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6759

European Commission (2019) "Questions and Answers – EU Cybersecurity." June 26, 2019. Accessed April 17, 2023 - https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369

European Commission (2022) "Questions and Answers: EU-U.S. Data Privacy Framework, draft adequacy decision." December 13, 2022. Accessed April 16, 2023 - https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632

European Data Protection Board (2023) "EDPB Welcomes Improvements under the EU-U.S. Data Privacy Framework, but concerns remain." February 28, 2023. Accessed April 16, 2023 - https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en

European Parliamentary Research Service (2020) "BRIEFING: Digital Sovereignty for Europe." *EPRS Ideas Paper* July 2020: 1-12.

Finnemore, Martha (1996) "Defining State Interest." In *National Interests in International Society*, 1-33. Ithaca: Cornell University.

Gao, Xinchuchu (2022) "An Attractive Model? China's Approach to Cyber Governance and Its Implications for the Western Model." *The International Spectator* 57 (3): 15-30.

Geller, Anja (2020) "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective." *GRUR International* 69 (12): 1191-1203.

Ghiasy, Richard and Rajeshwari Krishnamurthy (2021) "China's Digital Silk Road and the Global Digital Order." *The Diplomat*, April 13, 2021. Accessed April 1, 2023 - https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/

Glasze, Georg et at (2022) "Contested Spatialities of Digital Sovereignty." *Geopolitics* 28 (2): 919-958.

Global Freedom of Expression (na) "Google Spain SL v. Agencia Espanola de Protección de Datos." *Columbia University*. Accessed April 14, 2023 - https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/

Gray, Joanne (2021) "The Geopolitics of 'Platforms': the TikTok Challenge." *Internet Policy Review* 10 (2): 2-26.

Greene, Robert and Paul Triolo (2020) "Will China Control the Global Internet Via its Digital Silk Road?" *Carnegie Endowment for International Peace,* May 8, 2020. Accessed April

1, 2023 - https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

Hurd, Ian (2008) "Constructivism." In *The Oxford Handbook of International Relations*, 298-316. Edited by Christian Reus-Smith and Duncan Snidal. New York: Oxford University.

Internet Communication Magazine (2018) "'One Belt, One Road' Digital Economy International Cooperation Initiative Released." *Cyberspace Administration of China*, May 11, 2018. Accessed April 2, 2023 - http://www.cac.gov.cn/2018-05/11/c_1122775756.htm

Kawakami, Takashi et al (2023) "Huawei's Rebirth as Cloud Provider Faces Total U.S. Export Ban Threat." *Nikkei Asia*, March 3, 2023. Accessed April 10, 2023 - https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-rebirth-as-cloud-provider-faces-total-U.S.-export-ban-threat#:~:text=The%20U.S.%20Commerce%20Department%20first,government%20could%20access%20sensitive%20data.

Lambach, Daniel (2020) "The Territorialization of Cyberspace." *International Studies Review* vol. 22: 482-506.

Lin, Xiaofeng (2020) "A Dangerous Game: China's Big Data Advantage and How the US Should Respond." *Journal of Law, Technology and Policy* vol. 2020 no. 1: 253-281.

Liu, Lizhi (2021) "The Rise of Data Politics: Digital China and the World." *Studies in Comparative International Development* vol. 56: 45-67.

Lynskey, Orla (2015) "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez." *The Modern Law Review* 78 (3): 522-548. P. 523.

Mearsheimer, John J. (2001) The Tragedy of Great Power Politics. New York: W. W. Norton.

Ministry of Foreign Affairs of the People's Republic of China (2020) "Global Initiative on Data Security." *MFA of the PRC*, September 8, 2020. Accessed April 20, 2023 - https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html

Morgan, Hani (2021) "Conducting a Qualitative Document Analysis." *The Qualitative Report* 27 (1): 64-77.

Morgenthau, Hans J. (2005 [1948]) *Politics Among Nations*. Seventh Edition revised by Kenneth W. Thompson and W. David Clinton. Boston: McGraw-Hill.

Nussipov, Adil (2020) "Data Governance in America: Between the Silicon Valley Consensus and California's Privacy Rules." *Center for Media, Data and Society*, February 10, 2020. Accessed April 10, 2023 - https://medium.com/center-for-media-data-and-society/data-governance-in-america-between-the-silicon-valley-consensus-and-californias-privacy-rules-f78cb8619008

Okumus, Serra (2022) "The Rising Political Power of Silicon Valley." *Fiker Institute*, April 2022. Accessed April 10, 2023 - https://www.fikerinstitute.org/publications/the-rising-political-power-of-silicon-valley

Parasol, Max (2018) “The Impact of China’s 2016 Cyber Security Law on Foreign Technology Firms, and on China’s Big Data and Smart City Dreams.” *Computer Law and Security Review* vol. 34: 67-98.

Paszak, Pawel (2020) “China’s Growing Influence in International Organizations.” Warzaw Institute, October 14, 2020. Accessed April 2, 2023 - https://warsawinstitute.org/chinas-growing-influence-international-organizations/

Rose, Gideon (1998) ”Review: Neoclassical Realism and Theories of Foreign Policy.” *World Politics* 51 (1): 144-172.

Starman, Adrijana Biba (2013) “The Case Study as a Type of Qualitative Research.” *Journal of Contemporary Educational Studies* vol. 1: 28-43.

State of California Department of Justice (2023) “California Consumer Privacy Act (CCPA).” February 15, 2023. Accessed April 15, 2023 - https://oag.ca.gov/privacy/ccpa

The European Parlement [EP] & The Council of the European Union [EUCO] (2016) ”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).” *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

The Information Office of the State Council of the People’s Republic of China (2010) “The Internet in China.” *China Daily*, June 8, 2010. Accessed March 28, 2023 - https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm

The National People’s Congress of the People’s Republic of China (2021) “Data Security Law of the People’s Republic of China.” *NPC*, June 10, 2021. Accessed March 21 2023 - http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml

The National People’s Congress of the People’s Republic of China (2021) “Personal Information Protection Law of the People’s Republic of China.” *NPC*, August 20, 2021. Accessed March 21, 2023 - http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

The United States Department of Justice (2018) “CLOUD Act Resources.” Updated March 8, 2023. Accessed April 15, 2023 - https://www.justice.gov/criminal-oia/cloud-act-resources#:~:text=The%20CLOUD%20Act%20is%20designed,fight%20serious%20crime%20and%20terrorism.

The White House (2017) “National Security Strategy of the United States of America.” *Trump White House Administration*, 1-55 - https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

The White House (2022) “FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework.” *Biden White House*, October 7, 2022. Accessed April 16, 2023 - https://www.whitehouse.gov/briefing-

room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

The White House (2022) "National Security Strategy." *Biden-Harris White House Administration*, 6-48 - https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

Wendt, Alexander (1992) "Anarchy is What States Make of it: The Social Construction of Power Politics." *International Organization* 46 (2): 391-425.

Wendt, Alexander (1999) "Three Cultures of Anarchy." In *Social Theory of International Politics*, 246-312. Cambridge: Cambridge University.

Wood, Georgia and James Andrew Lewis (2023) "The CLOUD Act and Transatlantic Trust." *Center for Strategic and International Studies*, March 29, 2023. Accessed April 15, 2023 - https://www.csis.org/analysis/cloud-act-and-transatlantic-trust

World Bank (2021) *World Development Report 2021: Data for Better Lives*. Washington DC: World Bank.

Xinhua News Agency (2016) "Cyber Security Law of the People's Republic of China." *Cyberspace Administration of China*, November 7, 2016. Accessed March 27, 2023 - http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

Yamada, Atsushi (2000) "Neo-Techno-Nationalism: How and Why It Grows." Working Paper for *International Studies Association Convention*, March 14-18, 2000 - https://ciaotest.cc.columbia.edu/isa/yaa01/

Zhao, Xinying (2019) "Legislation Coming to Better Protect Personal Details, Spokesman Says." *China Daily*, March 4, 2019. Accessed March 22, 2023 - https://www.chinadaily.com.cn/a/201903/04/WS5c7cbaa4a3106c65c34ec9ae.html

Zuboff, Shoshana (2019*) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.