Exploring a Brave New World: Unpacking the Implications of China's Data Legislation

Word Count: 4978

NZLSA Paper Presentation Competition

Jaiden Tucker – Team D

I Introduction

China was a late player when it came to regulation in the data realm but since picking up the controller recently, it has implemented legislation quickly and systemically. This article assesses China's data regulation legislative framework, unpacking the legislation's direct ramifications both domestically and internationally, while also situating the legislation within broader data regulation trends. To do this, the article proceeds in four parts. Firstly, the context of data and legislation is conceptualised to explain the importance of data and how this shaped the Chinese approach. Secondly, this article explores a comparative view of personal information protection between China, the United States, and the European Union. Thirdly, the Chinese legislative trends are considered within a global trend of shifting from territoriality to extraterritoriality. Fourthly, the role of the Chinese legislative approach within the proliferation of digital authoritarianism is analysed. The analysis presented in these four parts provides a bleak projection for the future of the data realm as it trends towards facilitating repression and increasing superpower rivalry.

II Context

This section contextualises the broader analysis by introducing the significance of data, as well as how this has framed the Chinese legislative approach. I begin in this part with a discussion of data's economic and geostrategic dimensions, which assists in providing a background and establishing the significance of data to states in the modern age. This will help colour the second aspect of this part, where I explore the Chinese legislative framework.

A Data

Data, fundamentally, is a collection of information. It encompasses everything from healthcare information to national security secrets to weather records. The breadth of data is so immense, that in the modern technological age, it encapsulates the vast majority of the world around us. To further contextualise the utmost importance of data, this part will explore the economic and geostrategic dimensions of data.

1 Economic Dimension

Data's economic dimension has taken increasing precedence in mainstream media attention, with analogies drawn to oil's economic centrality in the 20th Century.[1] However, data can be fundamentally distinguished from traditional resources, such as oil. Firstly, data is not a finite resource in the same measure as traditional material resources.[2] A barrel of oil, once consumed, has no ability to provide future utility. Comparatively, data can be used infinitely without any derogation in its quality. This quality creates the second notable feature, which Agrawal

[1] Kiran Bhageshpur "Data Is The New Oil—And That's A Good Thing" *Forbes* (online ed, New Jersey, 15 November 2019).
[2] Hal Varian "Artificial Intelligence, Economics, and Industrial Organization" in Ajay Agrawal, Joshua Gans and Avi Goldfarb (eds) *The Economics of Artificial Intelligence: an Agenda* (The University of Chicago Press, Chicago, 2019) 399 at 405.

describes as increasing returns to scale.[3] This manifests itself in two key methods: data's recursive optimisation processes; and scalability through the combination with other production methods.[4] An example of this optimisation is Uber, where data creates an initially useful product that subsequently generates additional useful data which improves product. The scalability was explained by Liu in the context of Tesla, as self-driving technology requires the same technology to create one or a million self-driving cars.[5] Therefore, data lends itself to large-scale processes, where increasing collection and use of data requires little additional cost with great benefits.

2 Geostrategic Dimension

Data's role as a geostrategic asset draws from three key aspects. Firstly, the aforementioned economic aspect makes the control of data a method of economic competition between states.[6] Secondly, data has become prevalent in national security.[7] Finally, data allows for the maintenance of power through suppression of dissent in authoritarian states to a degree that has not been seen before.[8] This all-encompassing control of the systems of communication provides the ability to maintain political stability and silence the voices of dissidents. Overall,

---

[3] Ajay Agrawal, Joshua Gans and Avi Goldfarb *Prediction Machines: The Simple Economics of Artificial Intelligence* (Harvard Business Review Press, Boston, Massachusetts, 2018) at 230.
[4] Lizhi Liu "The Rise of Data Politics: Digital China and the World" (2021) 56 Studies in Comparative International Development 45 at 49.
[5] Liu, above n 4, at 50.
[6] Liu, above n 4, at 45. See also:
Jay Pil Choi, Doh-Shin Jeon and Byung-Cheol Kim "Privacy and personal data collection with information externalities" (2019) 173 Journal of Public Economics 113 at 115.
Yan Carriere-Swallow and Vikram Haksar "The Economics and Implications of Data: An Integrated Perspective" (2019) 18 IMF 1 at 15.
[7] Cambridge Analytica's data breaches resulted in threats to democracy in the United States and United Kingdom. See Colin J Bennett and David Lyon "Data-driven elections: implications and challenges for democratic societies" (2019) 8 Internet Policy Rev 1 at 2.
Trump's exclusion of Huawei was premised on the threat of the exposure of critical data to the Chinese government. See Daniel W Drezner "Economic Statecraft in the Age of Trump" (2019) 42 Wash. Q. 7 at 12.
[8] Sheena Chestnut Greitens "Authoritarianism Online: What Can We Learn from Internet Data in Nondemocracies?" (2013) 46 PS Polit Sci Polit 262 at 265.

data is an immensely critical geostrategic asset that may determine the international balance of power in the 21st century.

B Legislative Context

Chinese data law has rapidly developed in recent years and is now encompassed by three main Laws: the Cybersecurity Law (CSL) of 2016, the Data Security Law (DSL) of 2021 and the Personal Information Protection Law (PIPL) of 2021. These are "basic laws", which serve at the highest level of the Chinese legal pyramid. Together, these three pieces of legislation, combined with additional regulations, national codes and other extraneous pieces of legislation create a complex and detailed legislative framework.

1 Cybersecurity Law

The Cybersecurity Law (CSL) was the first of the major laws passed in this area. This functionally constrains network operators and protects both personal and critical information.[9] There are two important features to note about the CSL. Firstly, the CSL serves as a broad backbone. As noted by Qi, Shao & Zeng, "its basic function is to build China's cybersecurity legal system, not to solve any specific cybersecurity issues."[10] The second key feature is the purpose, which is prefaced by a focus on "ensur[ing] cybersecurity, to safeguard cyberspace sovereignty, national security...".[11] The inclusion of cyberspace sovereignty is specifically noteworthy, as this is a highly contested realm of digital law and the inclusion of this concept drew complaints from 46 international organisations during the drafting stage of the law.[12] The

[9] Aimin Qi, Guosong Shao and Wentong Zheng "Assessing China's Cybersecurity Law" (2018) 34 CLSR 1342 at 1343.
[10] Qi, above n 9, at 1344.
[11] 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China] 2017 (People's Republic of China), art 1.
[12] Qi, above n 9, at 1344.

CSL provides a basis for future legislation and regulations and sets the scene for the elevation of national security within data law rationale.

2 Data Security Law

The Data Security Law (DSL) focuses primarily on cybersecurity through creating a framework to classify data collection, storage and transfer. There are two key features of the DSL to note. Firstly, the law has a broad scope; with jurisdiction over both extraterritorial data and almost all data within China.[13] The second key feature is the categorisation system, which hierarchically classifies data and determines the protections which must be provided.. The two key categorisations of data are Important Data and National Core Data. Important Data is the second highest tier of data and is immensely unclear.[14] Core Data is a subset of Important Data and is the most sensitive tier of data. It is defined as data that regards national security and the public interest.[15] The most important obligations are contained in article 36, which prevents any data stored in China from being turned over to foreign judicial or law enforcement bodies without the express consent of the Chinese government, regardless of where the data was collected.[16] The DSL also imposes a raft of transfer, handling and security obligations upon data, with the most onerous for Core Data and Important Data. These include data localisation requirements, which forces Important Data to be stored in China, as well as onerous security requirements for overseas transfer.[17] Overall, the DSL provides a rigorous cybersecurity protection framework to uphold the Chinese national interest.

---

[13] 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China] 2021 (People's Republic of China), arts 2, 53, 54.
[14] Jihong Chen and Jiabin Sun "Understanding the Chinese Data Security Law" (2021) 2 Int Cybersecur Law Rev 209 at 211.
[15] Chen, above n 14, at 215.
[16] Data Security Law, above n 13, art 36.
[17] Chen, above n 14, at 215.

3 Personal Information Protection Law

The Personal Information Protection Law (PIPL) is the third cornerstone of the data protection framework, and it protects personal information. The PIPL provides more rights to data subjects, greater requirements for data security and mandatory data localisation when personally identifiable information exceeds a certain threshold.[18] There are three key features to note about the PIPL. Firstly, the scope of the PIPL is also extensive, providing extraterritorial jurisdiction and ambiguous definitions.[19] Secondly, data collection is allowed either with consent or in a situation of necessity.[20] Necessity is very ambiguous, which may provide discretion for Chinese authorities to encourage politically-motivated action, as discussed later in this article. Finally, the PIPL contains blacklisting provisions which serve to put up further walls between states. Article 42 of the PIPL allows the blacklisting of organisations that harm the Chinese public interest and Article 43 allows reciprocity of retaliation if foreign governments are discriminatory against China.[21] Overall, the PIPL covers the personal information area of data protection through imposing specific requirements on data handlers and processors.

4 Subordinate Regulations

Outside of this tripartite legislative net, there are a great deal of subordinate regulations which colour these laws. The full details of these go beyond the scope of this article, due to both the number of regulations and the complexity of application. However, an aspect to note is a tendency to overlap the PIPL and DSL.[22] This is demonstrative of a key trend: the centrality of

[18] Daniel Albrecht "Chinese first Personal Information Protection Law in contrast to the European GDPR" (2022) 23 Comput Law Rev Int 1 at 1.

[19] 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China] 2021 (People's Republic of China), art 3.

[20] Personal Information Protection Law 2021, above n 19, art 13.

[21] Personal Information Protection Law 2021, above n 19, arts 42-43.

[22] Rogier Creemers, 'China's Emerging Data Protection Framework' (2021) SSRN 1 at 18.

the Chinese national interest creating an overlap between personal information and national cybersecurity.

Overall, the three key pieces of legislation, combined with a myriad of regulations and national standards create a nearly all-encompassing net in the realm of data protection. There is often considerable overlap between these areas of law and the recency of these laws prevents substantial academic or judicial commentary on how this will be resolved. However, the key trends of extraterritoriality, expansive vague drafting and a focus on the protection of national security are all very apparent and provide clues for the future of Chinese law in this area.

III Comparative International Approach to Personal Information

China emerged as a late player in the regulation of personal information. This meant that Chinese regulation exists in a predefined environment, which has often been conceptualised as a spectrum between the American laissez-faire approach and the European Union's primacy of privacy.[23] This led to initial conceptions of Chinese regulation as striking a balance between privacy and commercial freedom.[24] However, the fundamental flaw in this, lies within the western-centric perspective of how law operates. As noted by Clarke, assessing Chinese law through the framework of western legal systems often leads to missing crucial pieces of the puzzle.[25] This article will posit that there are three separate rationales at play and each actor has taken a different prioritisation to each.

[23] Gregory Voss "Obstacles to Transatlantic Harmonization of Data Privacy Law in Context" (2019) 1 U Ill JL Tech & Pol'y 405 at 407.
[24] Emmanuel Pernot-Leplay "China's Approach on Data Privacy Law: A Third Way Between the US and the EU?" (2020) 8 Penn ST JL & Intl AFF, 49 at 49-52.
[25] Donald Clarke "Puzzling Observations in Chinese Law: When Is a Riddle Just a Mistake?" in Stephen Hsu (ed) *Understanding China's legal system: essays in honor of Jerome A Cohen* (New York University, New York, 2003) 93 at 93-96.

A European Union

The legislative approach to personal information in the EU's General Data Protection Regulation (GDPR) is very similar to the Chinese approach. This is perhaps not surprising, considering the situation in which the PIPL was drafted. Chinese academics proposed the EU model was followed and legislators noted they took considerable inspiration from foreign sources.[26] Many of the specific rights accessible under the PIPL are very identical to those found in the GDPR, including access, withdrawal of consent and rules around data collection.[27] Additionally, the extraterritorial scope of the PIPL also aligns with the GDPR's approach.[28] There are some minor differences in specific drafting, which generally tend to be characterised by a lack of specificity in the PIPL.[29] However, these effectively function to create very similar obligations and coverage. Some have conceptualised that this has resulted in an alignment with the EU, dismissing the notion of a marked difference in regulatory tilt.[30]

However, there are important and substantial differences in the underpinning rationales and objectives of the respective acts. The GDPR fundamentally serves to uphold individual privacy and the right to privacy has a central position, as noted in article 1 which denotes the act "protects fundamental rights and freedoms of natural persons".[31] Notably, the ideal of fundamental individual rights is a notion firmly entrenched in Western legal systems. The

[26] Wanshu Cong "The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics" (2021) 4019797 SSRN 1 at 7.
[27] Riccardo Berti "Data protection law: A comparison of the latest legal developments in China and European Union" (2020) 1 Eur J Privacy L & Tech 34 at 34-35.
[28] General Data Protection Regulation 2016 (European Union), art 4.
[29] Xu Junke and Tang Ying "Legal Protection of Personal Data in China" [2021] 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress 837.
[30] Samm Sacks *New China Data Privacy Standard Looks More Far-Reaching than GDPR* (Centre for Strategic and International Studies 2018) at 1.
[31] General Data Protection Regulation 2016 (European Union), art 1.

teleological Chinese system does not recognise rights in a similar manner, which necessarily prevents this similarity at a structural level.[32] The PIPL comparatively has a central focus of upholding national security, as noted above.[33] This fundamentally means ambiguities, edge cases, enforcement, and the future development of legal principles will differ, according to the different objectives of the laws. Specifically, in a European context, the individual right to privacy creates broader legal principles upholding the protection of personal information, while the Chinese system does not have recourse to this fundamental basis.

Overall, the current protections for personal information in China appear to be converging with those of the EU, however, the rationale of these protections differ, which may lead to a divergence in how edge cases are resolved and a different regulatory approach in the future.

B United States of America

Unlike China and the EU, the USA has no specific legislation to protect personal information. To set the scene, the Court of Justice of the European Union in *Schrems II* considered the personal information protections in the USA to be inadequate.[34] To explain why this is, the USA's convoluted patchwork of relevant legislation smattered across federal and state levels must be considered. At a federal level, Jamison notes eight different acts which all can have relevance to personal information, without any clear boundaries between them.[35] In addition to a lack of federal legislation, the USA also diverges from China and the EU in failing to have a federal agency dedicated to personal information protection.[36] In the absence of federal law,

[32] Junke, above n 29, at 19.
[33] Personal Information Protection Law 2021, above n 20, art 1.
[34] Note that inadequacy here is used as legal terminology, where an assessment of adequacy corresponds to enforceability in the EU legal context. Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)* ECLI:EU:C:2020:559 at [203].
[35] Shaun Jamison "Creating a National Data Privacy Law for the United States" (2019) 10 Cybaris Intell Prop L Rev 3 at 7-12.
[36] Jamison, above n 35, at 7.

some states have stepped in and implemented state law. In California, this looks like legislation that is modelled from the GDPR and has significant protections.[37] However, only half of all states have any form of protection and the degree of protection varies within these.[38] Moreover, even with the attempted state legislation, this serves as an inadequate protection of personal information for two key reasons. Firstly, the complexity and overlap between statutes makes attempted compliance difficult, as the extent of obligations is often unclear at best.[39] Secondly, access to legal recourse is far more difficult in an environment without obvious agencies or legislation that have jurisdiction over this area, making the determination of a pathway a substantial barrier to any recourse.[40] This issue with access to justice ensures that, even in the best case scenarios, the USA still has far more meagre personal information protection law.

In providing these limited protections, the USA is able to give priority to innovation within the data sphere. The same inadequacies in personal information protection allow for business models that rely on the use of data to prosper, meaning they often locate themselves within the USA to make use of the lack of restraint on innovation.[41] Ultimately, when this rationale is put against the EU focus on individual privacy and China's focus on the state interest, regulatory approaches to personal information can best be viewed as being pulled in three directions, rather than the initial conception of a spectrum.[42] The balancing of these three interests have been approached differently in each state, and in this way, China does serve as a third way.

[37] Paul Breitbarth "The impact of GDPR one year on" (2019) 1 Netw Secur 11 at 20.
[38] Jamison, above n 35, at 13.
[39] Jamison, above n 35, at 19.
[40] Jamison, above n 35, at 18.
[41] Tal Zarsky "The Privacy-Innovation Conundrum" (205) 19 Lewis & Clark L Rev 115 at 116.
[42] Zarsky, above n 41, at 116. See also: Dongsheng Zang "Revolt against the US Hegemony: Judicial Divergence in Cyberspace" (2022) 39 Wis Int'l L J 1 at 68; Masao Horibe "The Realization of Mutual Adequacy Recognition Between Japan and the EU and Issues Raised in the Process" (2020) 1 Global Privacy Law Review 145; Simon Gunst and Ferdi De Ville "The Brussels Effect: How the GDPR Conquered Silicon Valley" (2021) 26 Eur. Foreign Aff. Rev. 437.

C Discussion

When understanding the implications of these differing rationales, recourse to unpacking the normative justifications is needed. The American laissez-faire approach has been justified by reference to innovation, however the continuation of innovation in the EU after the GDPR's implementation gives rise to the question of whether the type of additional innovation is normatively desirable.[43] Given data protection in Europe and China relies upon principles such as consent and knowledge, the type of innovation that may be excluded by increased regulation are perhaps less legitimate. Additionally, the logic of increased innovation is perhaps flawed as well. A recent study has claimed that the GDPR increases business activity due to growing public trust, which creates more engagement and economic activity.[44] This means that the laissez-faire approach may not even provide additional innovation and any increased innovation is unlikely to be morally desirable.

The Chinese approach of prioritisation of state interests is difficult to address through a western conception of law. This approach doubtlessly ensures the stability of the state, which is positive through a statist lens which has been coloured by a Confucian national identity. However, through a western liberal conception, this approach allows for governmental repression and limits the ability of vulnerable individuals to seek recourse against the immense power of the state. Considering the increasing power imbalance due to powerful data collection and technological centrality to society, protection of private information also allows for the protection of a sense of the individual. Overall, the focus on an individual's right to privacy upholds rights which are under siege.

[43] Zarsky, above n 41, at 118.
[44] Capgemini Consulting *Seizing the GDPR Advantage: From mandate to high-value opportunity* (2018) 1 at 1-10.

IV Data Sovereignty

A notable trend occurring within the data realm is the transition from data sovereignty and territoriality towards extraterritoriality.[45] To explain this movement, this article will firstly contextualise the initial rise of data sovereignty as a method to maintain a degree of control over the internet. Secondly, this article will address the international trends towards extraterritorial reach and situate the Chinese legislation in the context of the EU and USA. Finally, the consequences of jurisdictional overlap will be addressed, with particular focus on the likelihood of increasing superpower rivalry. Overall, this will demonstrate the influence of China's data legislation in the shift towards extraterritoriality and its consequential soft conflict.

A Context

In the early days of the internet, it was held out to be a space beyond traditional conceptions of Westphalian sovereignty, being optimistically conceptualised as a space beyond the reach of governments.[46] This optimism quickly faded as regulatory controls began to catch up.[47] Initially, this occurred in the form of American hegemony.[48] As a key early actor in this sphere, the USA both shaped a lot of discourse around the international constraints on the internet and was where a large amount of infrastructure was actually located. [49] As other countries caught up, this domination by the USA gave way to a contested international space. Data sovereignty quickly became a natural remedy to the lack of certainty and control states managed to exercise

[45] Cong, above n 26, at 1.
[46] Yu Hong and G Thomas Goodnight "How to think about cyber sovereignty: the case of China" (2020) 13 Chin J Commun 8 at 9-10.
[47] Si Chen "Application of US Long-Arm Jurisdiction in Cross-Border Data Flows and China's Response" (2022) 19 UCLR 65 at 66.
[48] Chen, above n 47, at 66.
[49] Chen, above n 47, at 66.

over the internet.[50] This form of data sovereignty mostly faced inwards, controlling access and use of the internet within a state.[51] Perhaps the most famous example of this is the Chinese great firewall, which massively constrained the access to the internet.[52] However, territorialisation of the internet is typically not this extreme, with legislative controls allowing governments to control the actors within their states online existing as a far less extreme and more common form of data sovereignty.[53] Simply put, this was enabling governments to enforce laws over situations involving the internet. While the territorialisation of the internet has been primarily actioned through internal control, especially in China, internationally there has been a greater focus on extraterritorial control.

B International Trends

1 United States of America

The initial use of the internet to exert extraterritorial control happened primarily from the United States, in a stark contrast to their approach to personal information. The traditional approach has been characterised by Chen as "[a gradual extension of] the tentacles of its long-arm jurisdiction to the entire world".[54] The modern trends in the approach to extraterritoriality in the American legislature and judiciary has been disputed. On one hand, the USA has passed the Clarifying Lawful Overseas Use of Data Act (hereafter the "Cloud Act") in 2018, which granted a substantial degree of long-arm extraterritorial reach.[55] Chen has relied upon this to characterise the USA as expansionary and attempting to further this long-arm jurisdiction.[56]

[50] Hunter Dorwart "Data Governance in China: Emerging Trends for the Next Decade" (2020) 4005414 SSRN 1 at 12.
[51] Dorwart, above n 50, at 13.
[52] Dorwart, above n 50, at 13.
[53] Nicholas Tsaugourias "Law, Borders and the Territorialisation of Cyberspace" (2018) 15 IJIL 523 at 549.
[54] Chen, above n 47, at 65.
[55] Clarifying Lawful Overseas Use of Data Act 2018 (United States) Pub.L. 115–141 § 2523.
[56] Chen, above n 47, at 68.

On the other hand, Cong has looked primarily at the judiciary to depict the USA as contracting into an isolationist approach.[57] In *Kiobel v Shell*, which was not a cross-border data case but rather a private international tort case, the United States Supreme Court held there was a presumption against extraterritoriality.[58] Cong used protectionist policies in the cross-border data sphere to back up this claim, through looking at the decisions to block Huawei and TikTok from American soil.[59] When assessing these competing narratives, Chen's arguments appear more compelling because the introduction of legislation provides a clear indication of intent, while Cong erroneously assumes that internal protectionism must be divorced from continual extraterritoriality. There probably is a continuing focus on extraterritoriality from the USA and even if there is an intent to constrain their long-arm jurisdiction, it has not been clearly conveyed to other states.

2 European Union

When looking at the trends in the EU, a useful starting point is the extraterritorial provisions in the GDPR, which was noted above to be very similar to the PIPL. There are a range of extraterritorial measures afforded under the GDPR, which allows for a large degree of long-arm jurisdiction.[60] However, at a judicial level, there has been a restrained approach to these provisions. In *Google v CNIL*, it was held that the extent of the right to be forgotten is confined to the territorial boundaries of the EU.[61] This must be contrasted against the political backdrop, where the lack of homogeneity underpinning the EU leads to a somewhat conflicting political approach.[62] Currently, a balance is attempting to be struck between factions who prioritise the

[57] Cong, above n 26, at 14.
[58] *Kiobel v. Royal Dutch Petroleum Co.*, 569 US 108 (2013).
[59] Cong, above n 26, at 15.
[60] General Data Protection Regulation 2016 (European Union), art 4.
[61] Case C-507/17 *Google LLC v CNIL* ECLI:EU:C:2019:15 at [62]-[66].
[62] Theodore Christakis "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy" [2020] SSRN 1 at 65.

upholding of rights of EU citizens, which requires extraterritoriality and global regulatory leadership to maximise the extent of this, and an increasingly protectionist wing that wants to ensure territorial control at the cost of extraterritorial jurisdiction.[63] This is ultimately quite similar to the USA, in that the EU is dabbling with extraterritoriality, without a clear lighthouse indicating where the future regulatory pathway will develop.

3 China

As characterised earlier in this article, the Chinese legislation in this area arose late in the game. Therefore, this backdrop of an international trend towards extraterritoriality, or at least an apparent inclusion of long-arm jurisdiction, would have been relevant in the drafting process. Indeed, a Chinese professor Zhang Xinbao (translated by Cong), commented on the PIPL draft that "the bill should be acceptable to the EU and meanwhile not make China lose comparative advantage to the US".[64] The focus on comparative advantage between the USA and China is demonstrative of the perceived advantages of American extraterritorial jurisdiction and the necessity to counter this. When reconsidering the relevant aspects of Chinese legislation with this backdrop in mind, the entrenchment of extraterritoriality is clear. The PIPL and DSL both contain extraterritorial provisions, while the DSL also contains 'tripwire' provisions to counter extraterritorial claims from other states.[65] Overall, this creates an international environment where the major players of the USA, EU and China are all attempting to exert extraterritorial jurisdiction over each other.

---

[63] Cong, above n 26, at 14.
[64] Zhang Xinbao "Designing Personal Information Protection Framework should Take into Account the Role of Super Platforms" *Southern Metropolis Daily* (29 October 2020) <www.sohu.com>., as cited in Cong, above n 26 at 16.
[65] Creemiers, above n 23, at 13-15.

C Consequences of Jurisdictional Overlap

In an environment with significant jurisdictional overlap, an exertion of extraterritorial jurisdiction may lead to cascading attempts to undermine other states. Firstly, the rationale of why overlap is likely to be exercised can be explained through the increasing geopolitical leveraging of data and the likelihood for regulatory imitation. As discussed earlier in this article, there is significant geopolitical value to the control of data, so any state's attempt to exert control over data will provide them with a relative advantage. This creates an incentive on each state to react to any extraterritorial claims in an equivalent manner to maintain their own geostrategic position.[66] Secondarily, this incentive applies perversely to responsive machinery to create a system of regulatory imitation in the mould of a security dilemma in the paradigm of realist international relations thought. Simply put, new legislation that gives increased powers in responding to other states increases the ability to exercise control over data. This reduces the relative position of other states, unless they follow suit. Every time a state uses responsive data legislation, it is encouraging a regulatory race between competing states to optimise the ability to control data internally and externally.[67] This is particularly pernicious due to the uncertainty as to whether other states will exercise the full extents of their capabilities under their legislation, which enhances the risk of escalation. This will likely create a system where substantial and increasing extraterritorial control is the norm.

Notably, jurisdictional overlap is likely to eventuate in soft conflict to some degree, even if steps are taken to mitigate this. As demonstrated by the recent embargo trade war, the USA and China cannot be relied on to take actions which can benefit both states, when a relative

[66] Ben Buchanan *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford University Press, Oxford, United Kingdom, 2016) at 41.
[67] Buchanan, above n 66, at 48.

advantage may be up for grabs.[68] However, even in the instance without a large conflict arising between states, geopolitical agitation is still a likely outcome. An example of this may occur through "slippage", of which a key possibility is overlap between the PIPL and GDPR.[69] If the EU refuses to consider the PIPL as adequate, it may encourage China to utilise its retaliatory provisions regarding judicial discrimination, a possibility contemplated by Cong.[70] He continued to summarise the possible situation as how "regulatory tensions driven by economic interests (or other normative principles) can slip into geopolitical confrontations".[71] Effectively, even in the absence of a single large spark of conflict, small consistent agitations are likely to escalate and combine with other geopolitical issues to escalate superpower conflict.

A second consequence of increased extraterritorial jurisdiction is through the economic dimension of data. This issue was contemplated by Liu, who noted that these increased legal requirements function as "a new form of nontariff trade barrier for multinationals".[72] Notably, these barriers are not intended to uphold rights of individuals but rather to serve protectionist states attempting to get an advantage over other states. This contrasts from the legal barriers in the personal information section of this article which upholds personal privacy, which is a positive externality. An example of this is when the CSL required Apple to localise and store data in China, it only served to increase compliance cost, which got passed on to consumers.[73] Ultimately, the trend towards extraterritoriality not only increases the likelihood for

[68] Wei Shi "The Cat and Mouse Saga Continues: Understanding the US-China Trade War" (2020) 55 Tex Int'l L J 187 at 219.
[69] Cong, above n 26, at 16.
[70] At 16.
[71] At 16.
[72] Liu, above n 4, at 47.
[73] Liu, above n 4, at 44.

superpower rivalry but also increases compliance costs for multinationals, which directly harms consumers.

V Proliferation of Digital Authoritarianism

A fundamental characteristic of the Chinese legislative coverage is consistent and substantial recourse to the national interest as a fundamental principle.[74] The construction of legislation aimed primarily at empowering national interests in turn empowers authoritarianism, both internally and in the international proliferation of what has been coined digital authoritarianism. In this part, this article will demonstrate how China's legislative framework has assisted in the export of digital authoritarianism in the global south, before assessing the ramifications of this phenom. In doing so, it will note that the negative aspects of the Chinese approach are likely to be adopted in the global south, which massively increases the scale and severity of this article's analysis.

A Spreading Authoritarianism

Proliferation of China's perspective upon data can be primarily viewed through two key categories: technological development initiatives and influencing norms. China's legislative approach sits firmly within the influence of norms; however, the development initiatives will also be explained in this article to paint a full picture of the overall effect.

1 Development

The central project in the Chinese attempt to exert soft power internationally is the Belt and Road Initiative (BRI) and the technological aspect of this has been coined the Digital Silk Road

[74] Dorwart, above n 50, at 38.

(DSR).[75] China has positioned itself to be central in telecommunications through developmental outreach in the global south, particularly Africa.[76] At an infrastructural level, Huawei has developed the vast majority of cellular data networks in Africa, while China Telecom is planning on providing fibre optic cable to nearly 50 African states.[77] At a consumer level, Transsion Holdings is the leading smart phone provider in Africa and Hikvision provides thousands of security cameras in South Africa.[78] Finally, at a policy level, Chinese companies have positioned themselves in advisory positions.[79] A key example of this is Huawei being the principal advisor for the Kenyan telecommunications "master plan".[80] Overall, Chinese companies have deeply ingratiated themselves in systems of telecommunications in the global south and at multiple levels.

2 Norms

While the developmental initiatives explain how China exercises control, it doesn't demonstrate how the spread of authoritarianism is specifically likely. This is where the indirect normative interactions are critical. Previously, the 'Brussels Effect' has been of notable influence, where having a clear option to model the approach from EU legislation and the ability to interact with a large market has allowed states to adopt this approach.[81] Having an alternative legislative approach from China developing recently, in combination with the economic dependency on China and similar constitutional arrangements, may lead to a

---

[75] Guo Huadong "Steps to the digital Silk Road" *Nature* (30 January 2018) <www.nature.com>.
[76] Willem Gravett "Digital neo-colonialism: The Chinese model of internet sovereignty in Africa" (2020) 20 Afr Hum Rights Law J 1 at 2.
[77] David Ignatius "China has a Plan to Rule the World" *The Washington Post* (29 November 2017) <www.washingtonpost.com>.
Amy Mackinnon "For Africa, Chinese-Built Internet Is Better Than No Internet at All" *Foreign Policy* (19 March 2019) <https://foreignpolicy.com>.
[78] Willem Gravett "Digital Coloniser? China and Artificial Intelligence in Africa" (2020) 62 Survival 153 at 156.
[79] Gravett, above n 76, at 3.
[80] Michael Abramowitz and Michael Chertoff "The global threat of China's digital authoritarianism" *The Washington Post* (1 November 2018) <www.washingtonpost.com>.
[81] Anu Bradford "The Brussels Effect" (2012) 107 NW U L Rev 1 at 1-3.

continual trend towards data authoritarianism in the global south.[82] In terms of constitutional arrangements, due to colonialism, governmental instability in the global south is fairly endemic.[83] This leads itself towards authoritarian tendencies in many states and this makes the Chinese model of national interest primacy very attractive.[84] Many African states have copied China's approach by shutting down access to social media in light of weakening stability, such as Chad closing down the internet for 16 months in light of discontent or Sudan shutting down the internet before a massacre of dissidents to prevent information spreading on social media.[85] An explicit example of how this has directly influenced legislation is in Zimbabwe, where the government directly espoused how the Chinese internet model was one to be followed and have continued down a repressive pathway.[86] Overall, the Chinese legislative approach has created a dispersive effect due to the underpinning rationale being closer to the constitutional arrangement of weak states in the global south.

B Ramifications

The Chinese approach to legislation and fostering authoritarianism in the global south makes the maintenance of authoritarianism far more likely.[87] The proliferation of authoritarianism is an immense harm and western liberal democracies should be taking a far more active role to intervene in this area. Secondly, a question has been raised as to whether the data sovereignty this approach is attempting to create in the global south is actually illusory.[88] The substantial reliance upon the Chinese state either directly through developmental aid, or indirectly through

---

[82] Matthew S Erie and Thomas Streinz "The Beijing Effect: China's Digital Silk Road as Transnational Data Governance" (2021) 54 NYU J Int'l L & Pol 1 at 14.
[83] Johan Lagerkvist "Chinese eyes on Africa: Authoritarian flexibility versus democratic governance" (2009) 27 J Contemp Afr Stud 119 at 120.
[84] Lagerkvist, above n 83, at 122.
[85] Lagerkvist, above n 83, at 123.
[86] Charity Wright "China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road" (2021) 41 SAIS Rev Int Aff 89 at 102.
[87] Wright, above n 86, at 104.
[88] Erie and Streinz, above n 82, at 5.

the power exercised over Chinese corporations, means that even in states which are attempting to develop away from authoritarianism, China maintains a great degree of control over the state.[89] Overall, China's legislative framework arguably goes a long way towards expanding and entrenching the influence of authoritarianism in the global south. This has the possible impact of legitimising authoritarian power to a greater degree globally or creating a network of influence so vast that support is basically guaranteed.[90] In turn, this is fundamentally important in terms of protecting and upholding the security of the Chinese state.

VII Conclusion

Trying to understand and predict trends in the data realm is a bit like finding a needle in a haystack, if the haystack was exponentially increasing in size and complexity at a daily rate. However, what this article does attempt to do, is decipher China's actions in a holistic context to unpack the underpinning themes. In doing so, certain trends can be identified, and potential ramifications can be explored. This article demonstrates that the legislative framework laid down by China paves a new direction in the realm of personal information, while generally pushing international data towards extraterritoriality and pursuit of the national interest. Ultimately, China's actions in this sphere should be of great alarm for western liberal democracies and a proactive approach is required to counter China's growing influence domestically, regionally, and internationally.

[89] Erie and Streinz, above n 82, at 82-3.
[90] Daniëlle Flonk "Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control" (2021) 97 Int Aff 1925 at 1927.

VIII Bibliography

A Cases

1 European Union

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)* ECLI:EU:C:2020:559

Case C-507/17 *Google LLC v CNIL* ECLI:EU:C:2019:15

2 United States

Kiobel v. Royal Dutch Petroleum Co., 569 US 108 (2013).

B Legislation

1 China

Administrative Measures for Data Security (Draft for Comment) 2019.

Cybersecurity Law 2017.

Data Security Law 2021.

Personal Information Protection Law 2021.

2 European Union

General Data Protection Regulation 2016.

3 United States

Children's Online Privacy Protection Act 1998.

Clarifying Lawful Overseas Use of Data Act 2018.

C Books and Chapters in Books

Ajay Agrawal, Joshua Gans and Avi Goldfarb *Prediction Machines* (Harvard Business Review Press, Boston, Massachusetts, 2018).

Ben Buchanan *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford University Press, Oxford, United Kingdom, 2016).

Donald Clarke “Puzzling Observations in Chinese Law: When Is a Riddle Just a Mistake?” in Stephen Hsu (ed) *Understanding China’s legal system: essays in honor of Jerome A Cohen* (New York University, New York, 2003) 93.

Jeremy Garlick *The Impact of China’s Belt and Road Initiative* (1st ed, Routledge, London, 2019).

Hal Varian “Artificial Intelligence, Economics, and Industrial Organization” in Ajay Agrawal, Joshua Gans and Avi Goldfarb (eds) *The economics of artificial intelligence: an agenda* (The University of Chicago Press, Chicago, 2019) 399.

D Journal Articles

Brett Aho and Roberta Duffield “Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China” (2020) 49 Economy and Society 187.

Daniel Albrecht “Chinese first Personal Information Protection Law in contrast to the European GDPR” (2022) 23 Comput Law Rev Int 1.

Christopher Balding “The Case Against Huawei” (2020) 3519948 SSRN 1.

Colin J Bennett and David Lyon “Data-driven elections: implications and challenges for democratic societies” (2019) 8 Internet Policy Review.

Riccardo Berti “Data protection law: A comparison of the latest legal developments in China and European Union” (2020) 1 Eur J Privacy L & Tech 34.

Anu Bradford “The Brussels Effect” (2012) 107 NW U L Rev 1.

Paul Breitbarth “The impact of GDPR one year on” (2019) 2019 Netw Secur 11.

Federico Caprotti and Dong Liu “Platform urbanism and the Chinese smart city: the co-production and territorialisation of Hangzhou City Brain” (2022) 87 GeoJournal 1559.

Yan Carriere-Swallow and Vikram Haksar “The Economics and Implications of Data: An Integrated Perspective” (2019) 18 IMF Departmental Papers.

Madison Cartwright “Internationalising state power through the internet: Google, Huawei and geopolitical struggle” (2020) 9 Internet Policy Rev 1.

Anupam Chander and Haochen Sun “Sovereignty 2.0” (2022) 55 Vand J Transnat’l L 283.

Jihong Chen and Jiabin Sun “Understanding the Chinese Data Security Law” (2021) 2 Int Cybersecur Law Rev 209.

Chen Si “Application of U.S. Long-Arm Jurisdiction in Cross-Border Data Flows and China’s Response” (2022) 19 UCLR 65.

Jay Pil Choi, Doh-Shin Jeon and Byung-Cheol Kim “Privacy and personal data collection with information externalities” (2019) 173 Journal of Public Economics 113.

Theodore Christakis “‘European Digital Sovereignty’: Successfully Navigating Between the ‘Brussels Effect’ and Europe’s Quest for Strategic Autonomy” [2020] SSRN 1.

Stephen Cody “Dark Law on the South China Sea” (2022) 23 Chic J Int Law 62.

Wanshu Cong “The Spatial Expansion of China’s Digital Sovereignty: Extraterritoriality and Geopolitics” (2021) 4019797 SSRN Electronic Journal 1.

Rogier Creemers “China’s Emerging Data Protection Framework” [2021] SSRN.

Tara Davenport “Island-Building in the South China Sea: Legality and Limits” (2018) 8 AsianJIL 76.

Hunter Dorwart “Data Governance in China: Emerging Trends for the Next Decade” (2020) 4005414 SSRN 1.

Daniel W Drezner “Economic Statecraft in the Age of Trump” (2019) 42 The Washington Quarterly 7.

Matthew S Erie and Thomas Streinz “The Beijing Effect: China’s Digital Silk Road as Transnational Data Governance” (2021) 54 NYU J Int’l L & Pol 1.

Daniëlle Flonk “Emerging illiberal norms: Russia and China as promoters of internet content control” (2021) 97 Int Aff 1925.

Zhiguo Gao and Bing Bing Jia “The Nine-Dash Line in the South China Sea: History, Status, and Implications” (2013) 107 American Journal of International Law 98.

Willem Gravett “Digital neo-colonialism: The Chinese model of internet sovereignty in Africa” (2020) 20 Afr Hum Rights Law J 1.

Willem Gravett “Digital Coloniser? China and Artificial Intelligence in Africa” (2020) 62 Survival 153.

Sheena Chestnut Greitens “Authoritarianism Online: What Can We Learn from Internet Data in Nondemocracies?” (2013) 46 PS: Political Science & Politics 262.

Simon Gunst and Ferdi De Ville “The Brussels Effect: How the GDPR Conquered Silicon Valley” (2021) 26 Eur Foreign Aff Rev 437.

Samantha Hoffman “China’s Tech-Enhanced Authoritarianism” (2022) 33 J Democr 76.

Yu Hong and G Thomas Goodnight “How to think about cyber sovereignty: the case of China” (2020) 13 Chin J Commun 8.

Masao Horibe “The Realization of Mutual Adequacy Recognition Between Japan and the EU and Issues Raised in the Process” (2020) 1 Global Privacy Law Review 145.

Shaun Jamison “Creating a National Data Privacy Law for the United States” (2019) 10 Cybaris Intell Prop L Rev 3.

Elizabeth K Kiessling “Gray Zone Tactics and the Principle of Non-Intervention: Can ‘One of the Vaguest Branches of International Law’ Solve the Gray Zone Problem?” (2020) 12 HLS National Security Journal 116.

James Kraska and Michael Monti “The Law of Naval Warfare and China’s Maritime Militia” (2015) 91 Int Law Stud 450.

Johan Lagerkvist “Chinese eyes on Africa: Authoritarian flexibility versus democratic governance” (2009) 27 J Contemp Afr Stud 119.

Jyh-An Lee “Hacking into China’s Cybersecurity Law” (2018) 53 Wake Forest L Rev 57.

Lizhi Liu “The Rise of Data Politics: Digital China and the World” (2021) 56 Studies in Comparative International Development 45.

Choon-ho Park “The South China Sea Disputes: Who owns the islands and the natural resources?” (1978) 5 Ocean Development & International Law 27.

Emmanuel Pernot-Leplay “China’s Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?” (2020) 8 Penn ST JL & Intl AFF, 49.

Aimin Qi, Guosong Shao and Wentong Zheng “Assessing China’s Cybersecurity Law” (2018) 34 CLSR 1342.

Athulasiri Kumara Samarakoon “Chinese Panopticon: Political Control of Cyberspace in China” (2009) 5 Vistas Journal of Humanities and Social Sciences 28.

Wei Shi “The Cat and Mouse Saga Continues: Understanding the US-China Trade War” (2020) 55 Tex Int’l L J 187.

Nicholas Tsaugourias “Law, Borders and the Territorialisation of Cyberspace” (2018) 15 IJIL 523.

Aysem Diker Vanberg “Informational privacy post GDPR – end of the road or the start of a long journey?” (2021) 25 Int J Hum Rights 52.

Gregory Voss “Obstacles to Transatlantic Harmonization of Data Privacy Law in Context” (2019) 1 U Ill JL Tech & Pol’y 405.

Christopher Walker “What Is ‘Sharp Power’?” (2018) 29 J Democr 9.

Charity Wright “China’s Digital Colonialism: Espionage and Repression Along the Digital Silk Road” (2021) 41 SAIS Rev Int Aff 89.

Tal Zarsky “The Privacy-Innovation Conundrum” (205) 19 Lewis & Clark L Rev 115.

E Reports

Capgemini Consulting *Seizing the GDPR Advantage: From mandate to high-value opportunity* (2018).

Hsin-hsuan Lin *Scientific and Technological Rights: A Panopticon Inside the Wall* (Taiwan Foundation for Democracy 2021).

Samm Sacks *New China Data Privacy Standard Looks More Far-Reaching than GDPR* (Centre for Strategic and International Studies 2018).

F Newspaper Articles

Michael Abramowitz and Michael Chertoff "The global threat of China's digital authoritarianism" *The Washington Post* (1 November 2018) <www.washingtonpost.com>.

John C Aquilino "China has fully militarized three islands in South China Sea, US admiral says" *The Guardian* (21 March 2022) <www.theguardian.com>.

Kiran Bhageshpur "Data Is The New Oil—And That's A Good Thing" *Forbes* (online ed, New Jersey, 15 November 2019).

Ron Cheng "Seizing Data Overseas from Foreign Internet Companies under the CLOUD Act" *Forbes* (29 May 2018) <www.forbes.com>.

Joseph Cox "I Gave a Bounty Hunter $300. Then He Located Our Phone" *Vice* (9 January 2019) <www.vice.com>.

Guo Huadong "Steps to the digital Silk Road" *Nature* (30 January 2018) <www.nature.com>.

David Ignatius "China has a Plan to Rule the World" *The Washington Post* (29 November 2017) <www.washingtonpost.com>.

Amy Mackinnon "For Africa, Chinese-Built Internet Is Better Than No Internet at All" *Foreign Policy* (19 March 2019) <https://foreignpolicy.com>.

RNZ "Chinese-built data centre in PNG exposed weakness" *Radio New Zealand* (12 August 2020) <www.rnz.co.nz>.

The Economist "In China, consumers are becoming more anxious about data privacy" *The Economist* (25 January 2018) <www.economist.com>.

Samuel Woodhams “How China Exports Repression to Africa” *The Diplomat* (23 February 2019) <https://thediplomat.com>.

Zhang Xinbao “Designing Personal Information Protection Framework should Take into Account the Role of Super Platforms” *Southern Metropolis Daily* (29 October 2020) <www.sohu.com>.