# Spear and Shield? — Legal Perspective on US and China's Approach to Data Sovereignty in the Big Data Era

Zhu (Judy) Zhu*

***Abstract*—In a world increasingly driven by advanced technologies, data have become "resources" that countries are competing for. This research paper addresses the question "what is the difference between the data strategies of the United States and China?". Existing literature has a provided comprehensive description of data sovereignty for both China and the United States, but they are usually standard doctrinal-comparative studies. However, this paper provides an additional historical dimension to the doctrinal comparisons. A framework of "spear and shield" is presented to describe how China's data strategy has evolved into a defensive mode while the United States holds an expansive data strategy. The research provides a new frame to understand the data competition between China and the U.S. among other countries. Similar kinds of methods could be utilized in other research on data strategies.**

***Keywords*—Data sovereignty, lawfare, technology and law, China and the United States**

## I. Introduction

This paper primarily discusses data sovereignty laws and strategies in both China and the U.S. It provides a framework of 'spear and shield' lawfare [1] to understand the strategic interactions between China and the U.S. in the field of data sovereignty and data transfer. Doctrinal, historical, and comparative methods are used in this research paper. By analyzing data legislations, regulations and emerging cases in China and the United States, the paper argues that the U.S. has an expansive data strategy, which will be referred to "spear" by trying to reach its extra-territorial data sovereignty through domestic regulations and multilateral agreements, while China adopts a more defensive data strategy-which refer to "shield" by localizing data and emphasizing data sovereignty and security within its borders.

Didi's case is a most recent embodiment of this 'spear-and shield' dynamics between the U.S. and China. Two days after Didi raised $4.4 billion from its New York initial public offering, China's regulatory agency Cyberspace Review Office launched a cybersecurity review based on the National Security Law and Cybersecurity Law because of Chinese security concerns whereby during the investigation new users' registration would be halted [2]. While China put measurements on data protection, the United States, on the other hand, was suspected of extracting foreign data through domestic law, namely, SEC requirement on auditing data from foreign firms according to the recently passed Holding Foreign Company Accountable Law (HFCAL) [3].

Manuscript received July 20, 2022; revised September 20, 2022; accepted December 20, 2022.

Zhu (Judy) Zhu is with United World College Southeast Asia, Singapore.
*Correspondence: zjudy1019@gmail.com.

This paper is divided into five parts. Firstly, the background and introduction will provide a short summary of the research. This will be followed by a brief literature review, which would build a foundation for the overall research. The strength and weaknesses, contributions and significance of this paper would be addressed in this section. It is followed by section 3 which discusses the evolution of data sovereignty lawfare between China and the United States. Section 4 provides a deep analysis of the recent and fiercely debated Didi case. In this section, the Chinese data strategy and United States data approach would be demonstrated and analyzed in detail. The paper then concludes.

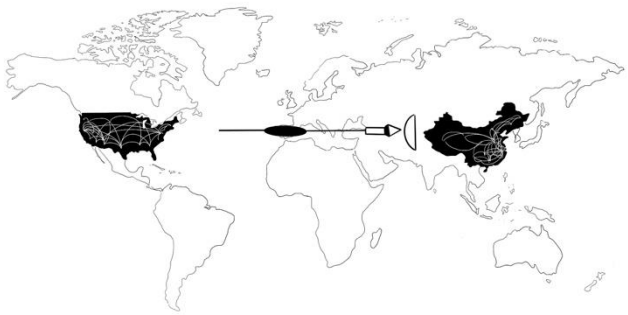

Fig. 1. "Spear" and "Shield" relationship.

### A. Big Data

According to IBM, "[B]ig data analytics is the use of advanced analytic techniques against very large, diverse big data sets that include structured, semi-structured and unstructured data, from different sources, and in different sizes from terabytes to zettabytes." [4] Big data is important because it could help governments and businesses to make decisions and make predictions.

### B. Data Sovereignty

Sovereignty is a political term, defined as the "supreme power, especially over a body politics" [5]. Cornell Law School [6] also defines sovereignty as "to have sovereign power is to be beyond the power of others to interfere." In terms of politics and international relations, state sovereignty is usually implied by territory boundaries. When the data era collides with sovereign ideals, however, a pivotal moment that challenges the definition of sovereignty arrived. Sovereignty over cyberspace is no longer constrained by territory borders. This created a great sensation in governments around the world because it is at this point of history where the state would reconsider its sovereignty

doi: 10.18178/ijssh.2023.13.1.1118

owing to the borderless nature of cyberspace and cross-border data flows. This scenario constitutes a new concept, namely "data sovereignty", meaning that the state has sovereign power over data. Nevertheless, the definition of data and what data belongs to which body politics, remain unanswered.

In the area of law, sovereignty is closely tied to the implementation of laws. This means that law can help the state to maintain sovereignty. Additionally, in the 21st century, law also has the capacity to expand sovereignty. In countries like the United States, the laws are implemented to expand U.S. data sovereignty over its borders. The Chinese state, on the other hand, tries to maintain its sovereignty within its borders, namely sticking to the traditional definition that keeping the data within the territorial boundary.

### C. Lawfare

Lawfare could be defined as using law as a weapon of war [7]. Nevertheless, in this paper, the concept of "lawfare" and how different countries use the law as "weapons" will be argued, even though the political relationship between China and the U.S. will not be discussed in great detail. China uses laws as a defensive "shield" to maintain data sovereignty, but the United States applies laws as an offensive "spear" to expand the sovereignty of data over the territory border.

### D. Spear and Shield

"Spear" is "a thrusting or throwing weapon with long shaft and sharp head or blade" [8], and "shield" could be defined as "a broad piece of defensive armor carried on the arm [9]. Seemingly, "spear" is offensive and "shield" is defensive. By applying the analogy of "spear and shield", this paper describes the conflicts between the U.S. and China's legal strategy of data sovereignty.

From the beginning of the internet era, evidence of the application of defensive strategy has been shown in China. It became more conspicuous in recent year when numerous data and cyber-related regulations and guidelines were implemented. For instance, the *Cybersecurity Review Measure* (CSRM) [1] provided measures for cybersecurity review if national security is suspected to be threatened. Additionally, Critical Information Infrastructure Regulations (CII Regulations)[2], a law implemented in 2021, specified the obligations of CII providers that were vaguely stipulated in the Cybersecurity Law (CSL). At the same time, Data Security Law (DSL)[3] and Personal Information Protection Law (PIPL)[4] were also enacted and will be effective in the coming month. To sum up, laws evolve to form a defensive "shield" where data sovereignty was maintained through prohibitive measures and acts.

On the U.S. side, the actions imply a more aggressive data strategy where the United States' domestic regulations gain extraterritorial effects in terms of data transfer, namely, "long-arm" jurisdiction. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[5] is a typical example in which domestic law in the United States evolved to have an extraterritorial legal effect. This law broadened the United States government's power over the data around the world as the users of transnational corporations like Facebook and Instagram are all around the world. Additionally, laws in the financial realm also show this phenomenon. SEC recently established the Holding Foreign Company Accountable Act (HFCAA)[6] as a snapshot of a larger offensive strategy where it requires data to be reviewed in foreign auditing firms, which in part extract data from firms that wanted to be listed in the U.S. stock market. Second, American multi-lateral agreements also play an expansive role in its data strategy of sovereignty and transfer. Most of the those mentioned above are components that make up America's expansive data strategy aiming to expand its data sovereignty.

## II. Literature Review

Investigating and researching the difference in strategies toward data sovereignty and potential conflicts is essential because data is viewed as a high-ranking resource as we enter the data era. However, before delving into the data part of the research, it is important to discuss the literature on internet regulation before the big data era. In *The Generative Internet* [10], Jonathan Zittrain described the nature of the internet as generative and ever-evolving because of the flexibility of code. This makes regulation arduous. One important argument he wanted to make is that with the limitation of law, generativity is sacrificed. He proposed that a balance of regulation and innovation is needed to be kept. For scholars like Joel R. Reidenberg, who made a proposal to the technology and internet jurisdiction [11], the balance between individual rights and internet jurisdiction is addressed. The existing legacy of internet jurisdiction and the rapidly-evolving nature of internet and data regulation urge the perception that more research needs to be done. After this, the data era approached where regulations and ownership were brought up one more time. Scholars also began to investigate those engaging questions.

In China, many scholars solely focused on the Chinese rationale for policymaking, commenting on the policies and proposing future frameworks. For example, on China's data localization [12], Jinhe Liu made a good explanation of the rationale of the Chinese approach to data sovereignty. On the legitimacy of data localization, Wang [13] made comments on the Chinese data mechanism of data sovereignty. Rooted in the unique Chinese safety-centered routes, he stated that, China should keep its localization mechanism but develop protective laws to enable future competition with other global powers. There were also scholars and organizations who provided people with a comprehensive study of the United States and the European Union's legislation on data sovereignty. For example, the U.S Department of Justice conveyed a clear image of the expansionist view through the CLOUD Act White Paper [14]. Additionally, a comparison

[1] Chinese Cybersecurity Review Measure. Translated version see https://www.chinalawtranslate.com/en/cyber-security-review/

[2] Critical Information Infrastructure Security Protection. Translated version see https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/

[3] Data Security Law. Translated version see https://www.chinalaw-translate.com/en/datasecuritylaw/

[4] Personal Data Protection Law. Translated version see https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

[5] Clarifying Lawful Oversea Use of Data Act(CLOUD Act). Full text see https://epic.org/privacy/cloud-act/cloud-act-text.pdf

[6] Holding Foreign Company Accountable Act. Full text see https://www.congress.gov/bill/116th-congress/senate-bill/945/text

between the Chinese data sovereignty strategy and the United States data sovereignty approach is a fiercely debated theme. John Selby [15] clarifies the underlying reason for the expansionist view which is the huge technology company based in the United States, and compares this with Chinese data localization. While these literatures are highly important for the foundation of this research topic, they lack a conceptual framework that could be expressed more adeptly and understandably for interpretation and analysis. This research includes secondary resources from international scholars including the early pioneers in the cyber law field. By including both Chinese literature and literature written by foreign researchers, this paper depicts a more comprehensive perspective on data sovereignty and its laws.

Furthermore, the application of this "Spear and shield" framework enables this paper to incorporate ideas from both political economy and international law & relations. Usually, scholars would analyze data sovereignty and data localization either from legal, political science, or international relations perspectives. Nevertheless, this research is able to provide a new perspective because interdisciplinary research is relatively rare in this novel field of data sovereignty and law. This model is also more understandable than merely listing the existing law and conflicts for both China and the United States.

Additionally, scholars mainly applied comparative methods to outline the distinction between the sovereignty approaches of China and the United States. While this is a beneficial method for the reader to have a clear view of the distinctions and similarities between different countries, the method lacks continuity by ignoring the overall formation and trend of the comprehensive legislation. In this essay, the historical method is used to elaborate from the beginning of the legislation regarding data sovereignty to the end. By understanding the past and the evolution timeline, readers would have a clearer view of how different strategies lead to different kinds of legislation. Finally, by analyzing the facts and distinctions between strategies according to the "Spear and Shield" framework, this paper enables the readers to have a clearer view of the distinction and similarities.

This paper is important because with increasing cases on data compliance and transfer around the globe, the spear-shield framework become helpful for analyzing future strategic interactions between major data powers not just between the U.S. and China but also including for example, between Europe and Africa. Practically, the analysis of existing laws and cases is also important for corporations to navigate through complex data compliance regimes. Politicians and policymakers could also look into the two different strategies when they draft their regulations. For other researchers, this research paper would enable them to gain insights that can be used to develop future comparative research, policy, legislation, and regulations with regard to different countries' data strategies.

## III. Evolution of the 'Spear and Shield' Dynamics

### A. Early Stage of Expansive U.S. Data Strategy

Following the 1980 Organization Economic Co-operation and Development (OECD) Guidelines, a few recommendations concerning cross-border data transfer for the improvement of the digital economy and data protection were addressed. [7] Under the OECD Guidelines, the council recognized the conflict between human rights protection and free data flow. Therefore, it provided space for member countries' interpretation by providing them with principles. European Union was among the first who responded to the Guidelines with the 1995 General Data Protection Regulation (GDPR), a comprehensive legal document that regards data protection as a fundamental right and solely focused on data-related issues.[8] Following the same guideline, however, the United States implemented her data protection law separately in different sectors [16]. Those legislative are usually in form of state laws and other means of regulation. Later, driven by the 1995 Data Protection Directive, the European Union and the United States signed the Safe Harbor to ensure the data flow between the two in order to keep healthy cross-border digital trade. Following that, the U.S. data strategy gradually appeared on people's horizons where the United States continued to stretch its sovereignty over data in the area of digital evidence collection after the 911 Attack when the Patriot Act was first implemented [17]. It was stated in Patriot Act that the data stored in US-based cloud service companies were subjected to U.S. government usage [18]. The U.S. government gradually increases the level of data extraction from the many U.S.-based companies [19]. According to Google's transparency report, the number of requests from U.S. officials had increased by 136% within three years from 2009 to 2012. This legislation builds upon the Safety Harbor framework and strengthens the government's authority over data [20]. Consequently, the Obama administration established the first big data plan by implementing the Big Data R&D Initiative which encourages six departments, investing 200 million, to develop the technology in the United States as a whole [17].

However, not much happened in the Eastern frontier. China was still in the stage of self-development while establishing a firewall to block western webpages. However, China wasn't absent from a new round of competition in the Big Data Era [12].

### B. Emerging "Spear" at the Western Front

When technology firms began to realize that the data produced on the internet are not "wastes", they began to take advantage of it by using them to make predictions and analyses. And this was the beginning of the Big Data Era. Before the government took data ownership into serious account, there was an abundance of businesses who utilized those personal data and made a great profit out of it. They usually sell those data to the third business to be predicted and make advertisements [21]. However, this underground activity gradually surfaced with Facebook Cambridge Analytica Scandal where Facebook mishandled over 50 million users' data to a political data analysis center Cambridge Analytica [22]. This analysis made with user's data was used for political advertisements. The government began to take action by fining heavily on Facebook.

However, not until the American Institution of the

[7] Organization Economic Co-operation and Development(OECD) Guidelines. Full text see https://www.oecd.org/sti/ieconomy/oecdguideline-sontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[8] General Data Protection Regulation. Full text see https://gdpr-info.eu

National Security Agency (NSA)'s unauthorized surveillance over personal devices around the world are revealed by Edward Snowden which involved a significant amount of governmental monitoring, did governments from many countries start to have serious sovereignty concerns over information and data they produced [23]. China responded by accelerating the implementation of data legislations [12]. And the European Union responded by intensifying the scrutiny over the United States' action because the EU viewed data privacy heavily because data privacy is a fundamental law according to GDPR. This was shown in a court ruling in 2015, the Court of Justice of the European Union (CJEU) invalid the Safety Harbor because of the inadequate data protection given by the U.S., proclaiming it was not in compliance with the principle of GDPR [24]. This court decision is primarily based on the Art. 45 of GDPR where an "adequate level of protection" is required to perform cross-border data transfer. However, events like Facebook Cambridge Analytica Scandal and NSA unauthorized surveillance over personal data post a skepticism over the U.S. data sovereignty issue. This was replaced by an agreement with a higher level of protection, namely Privacy Shield because both the European Union and the United States realized the importance of the cross-border economy which is dependent on cross-border data transfer.[9] At the same time, the EU strengthens its control over the US. Nevertheless, Privacy Shield was no longer valid because of the skepticism of lack of adequate data protection [25].

With the Trump administration, the United States turned to a more "selfish" state who urged to have more sovereignty. The United States was prompted to extract data from foreign countries by establishing bilateral and multilateral treaties dominated by the U.S. government in order to achieve data sovereignty. In order to become a "big brother" in the big data era, the United States also urged members of WTO to open up and establish free data flow [26]. In the Trans-Pacific Partnership (TPP) debate, the U.S. forcefully emphasizes the importance of cross-border data flow, and the U.S.'s agreement influences the agreement significantly as well. At the onset of this plan, the U.S. already started to enter agreements like the United States-Mexico-Canada Agreement (USMCA) where data localization was directly banned from the members of the agreement. No matter whether it is unauthorized surveillance or encouraging cross-border data transfer with the EU, the United States took a proactive stand on expanding sovereignty over data. Similarly, reflecting on the EU's response toward the U.S data strategy, U.S. expansive strategy was shown.

After the Microsoft case where the U.S. government demanded data stored outside of the U.S. from a multinational technology company, the CLOUD Act was established which amends the Stored Communication Act (SCA) of 1986 to extend the long-arm jurisdiction of the U.S .government. This ruling arouses international law-making to a new era where a New York State's ruling initiates a national law that influences international lawmaking, which is the so-called "international lawmaking 2.0" [27]. By implementing the CLOUD Act, the U.S. government hopes to propose the idea of "cross border data extraction" by stating that the government has access to foreign data collected by local businesses [28]. At the same time, according to the official explanation from the U.S. Department of Justice, the CLOUD Act not only applies to the U.S. registered corporate, but is also subject to Foreign firms who have a certain level of contact with the U.S. registered corporates, which means that foreign firms could easily get involved with regulation from the U.S. government. Additionally, with Facebook, Instagram and other transnational platforms becoming increasingly powerful in terms of data extraction and big data analysis, they operate more like a government [29]. With the massive data they obtained from billions of active users all around the globe, they have a huge amount of resources for valuable big data analysis. However, most of those global platforms are located in the U.S. where the CLOUD Act is implemented, creating an ideal environment for the U.S. government to perform data extraction.

Furthermore, the CLOUD Act has been marked as a turning point in the history of data sovereignty because if such a bilateral agreement would work, more countries would adopt the correspondent practice. This would potentially lead to borderless cyberspace, which means that the U.S. will have greater sovereignty over American users' data and potentially user's data over the world because the U.S. government may be able to extract data from an international internet company that is based in the United States according to the CLOUD Act 2018.[10] However, in reality, this bilateral legislative faces a difficult time implementing because many countries are struggling with the question of whether to take risks to be in an agreement with the U.S. with the danger of exposure of data from the country. European Union, Japan, and other countries have comprehensive data laws as they paced to the second generation of data protection legislations [30]. For example, GDPR has incorporated the elements of "data minimization", "data quality" and "data sensitivity" in the process of legislation. On the contrary, the United States legislations remain in the first generation which is based on OECD namely, it is still based on OECD which includes solely the fundamental privacy protections. Subsequently, many countries in the world don't support the CLOUD Act. Hence, the UK is the only country that signed the bilateral agreement since the inauguration of the CLOUD Act in 2018. Even though many countries are in the process of negotiating of joining the agreement, the paucity of agreements demonstrated that the United States' data strategy won a dearth of support. Not until 2018, similar legislation of GDPR, namely, the general data protection act was first established in the United States when the California Consumer Privacy Act (CCPA) passed.[11] However, this is just a state law which that has limited jurisdiction.

The United States, on the opposite, resembles a "spear" that has the aim to expand data sovereignty outside of the actual territory of the United States by implementing or enhancing domestic law and interfering with international order by establishing agreements between nations. Unlike

[9] Full text see https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_full_text.pdf.pdf

[10] CLOUD Act, U.S.C. §2713

[11] Full text see https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

China, the United States was proactive in the beginning stage of the data era where data was first being used on a massive scale by giving budget to develop big data [17].

Later, the ideology of overly gaining more sovereignty urges Trump administration to make a new move of limiting foreign technology companies and any form of possible extraction [26]. TikTok is an example of this. The Trump administration addressed the potential threat that data would be used by the Chinese government even though TikTok is registered as a U.S.-based company. As a result, the United States government still indicated that its sovereignty cannot be threatened by any means, showing the core of its expansionist ideology.

The European Union on the other hand gradually realized its lag in this data sovereignty battle. EU's awakening was presented by the invention of the concept of "digital sovereignty"-the EU version of sovereignty in the "data era". European digital sovereignty emerged as a result of the increase of the increasing dominance of non-European actors within the EU. During the global pandemic COVID-19, European Union was applying Apple and Google's tracking applications and those companies are U.S. based. However, this reduced Europe to a less favorable position in terms of data privacy. Digital sovereignty encourages the development and formation of European technology companies with the goal of maintaining sovereignty within the European Union, urging the European Union to be more proactive against foreign dominant firms. However, every move is rooted in GDPR and human rights protections, so we would not expect an expansive data strategy.

### *C. Emerging Shield: Chinese Data Strategy*

On the other hand, China was comparatively on the other side of the spectrum in terms of data strategy. From the previous political decision made by the Chinese government where the firewall was established within the Chinese border and additional blocking strategies, a conclusion could be made that the style and philosophy of politics in China were more conservative compared to the United States. According to Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information (1996) article 6 that "no units or individuals shall set up by themselves or use other access channels for international networking.", the Chinese government set a tone for the future development of data sovereignty. Additionally, "tall" fire does not signify China ceded this data sovereignty lawfare in the data era. A Chinese expert even commented that in this competition, the Western might be the closest to China in terms of the revolution of the internet-centered technology [19].

Criminal Law [10] was among the first law which criminalized the wrongdoing regarding data extraction. It was stated in article 285 that whoever "intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system", will be punished.

After the Snowden Leak and the growing amount of data produced by an exponentially growing number of internet users, China also realized that a national policy of data sovereignty needed to be established. Starting with Li Keqiang's "internet+" to the later 135 Plan where the new goal of China is to achieve better economic growth by making breakthroughs in informational technology, China officially realized that data sovereignty lawfare began, and joined the lawfare intending to maintain their data sovereignty in this data at the onset of the big data age. This era combines both the rapid development of data technology and followed laws that regulate data security in a world where data transmission occurs everywhere at any fraction of a second.

The Chinese way of data sovereignty was modeled on EU data localization with free flow of data within the country or group of countries and stricter rules when dealing with cross-border data. Before Cybersecurity Law (CSL), China has similar practices to the United States where laws regulating data transfer were scattered in many specific industries, multiple departments were overseeing data regulations in various areas [31]. In the early stage, transferring of data is regulated by article 17 of the Law of People's Republic of China on Guarding State Secrete which stated that "Measures for storing, drawing, processing and transmitting state secrets by electronic information and other technical means shall be formulated by the state secret-guarding department together with the central organs concerned." However, the definition of "state secret" remains ambiguous, articulated as "matters that have a vital bearing on state security and national interests and as specified by legal procedure, are entrusted to a limited number of people for a given period of time." According to this definition, a broad range of data could be included. In this case, we can see that China was gradually using regulations and national laws to seize its sovereignty over data by trying to keep it within the territorial boundary. A completely different story can be said in the United States where the government is not satisfied with the sovereignty it owned but uses international companies as a means to extend the sovereignty outside of its venue.

Not surprisingly, the establishment of CSL (2016) was a milestone of the Chinese's data sovereignty. It specified that "Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China" in Article 37, with the clarification that exceptions might occur "Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and information departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions." [12] Those two articles listed not only address the core values of data sovereignty in China which is to keep the data localized and perform security reviews. What's more, it also ensures healthy economic growth by allowing cross broader data transfer during the trading process. It is also denoted to safeguard "cyberspace sovereignty" in China. Interestingly, following the issue of CSL, American technology giant Apple moved their iCloud

[12] Cybersecurity Law. Act.37. Full text see https://www.newamerica.org/ cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peop- les-republic-china/

center for the personal information of Chinese citizens to Guizhou to comply with the CSL. Nevertheless, CSL was the only legislation regarding the internet and it is relatively incomplete due to deficiency of mentioning data protection and data security in terms of trans-border data flow directly. Besides, at the time when CSL came into effect, many key terms in CSL remain undefined. For example, what does it mean by Critical Information Infrastructure and what is included as CII are unclear.

Current CSL is not enough because there are international companies who are operating inside China that need to transfer data to the headquarter, and the firewall did not necessarily block Chinese citizen from accessing Facebook, Twitter, Instagram and YouTube because of technology, namely, Virtual Private Network (VPN). Additionally, trading internationally also requires data transfer from China to foreign countries. More comprehensive laws are needed for the Chinese legislative since interaction with foreign institutions is highly important to domestic economic development and a balance is needed between national interest, domestic development and privacy protection [32].

The beginning of the data laws implementation flux was the Cryptography Law which came into effect in 2019. In article 2 of Cryptography Law, the definition of cryptography was addressed, namely, "technologies, products and services utilized for encryption protection and security authentication on information and the like by using specific transformation methods." And the purpose of this law directly demonstrates China's defensive strategy, which is stated in article 1:

This Law is enacted for the purpose of regulating the application and administration of cryptography, promoting the development of cryptography work, ensuring cyber and information security, safeguarding national security and public interests, and protecting the legitimate rights and interests of citizens, legal persons and other organizations.

Later in 2020, more data laws and drafts are issued, polishing the 2014 CSL. Measures for Security Assessment of Cross-Border Data Transfer of Personal Information (For Public Comment) in 2019 made certain updates on the 2017 Measures for Security Assessment of Cross-Border Data Transfer of Personal Information and Important Data (For Public Comment). Multiple undefined terms in CSL are specified. They also promote strict assessment guidelines when cross-border data transfer is practiced. [13] Moreover, more drafts regarding data protection were issued, which build up upon the existing legislation regarding cross-border data transfer. Additionally, Draft Personal Information Protection Law (PIPL) was issued in 2020. This took Chinese cross-border data transfer legislation to the next level. PIPL (draft) also learned from Article 45 of GDPR which "adequate level of protection" is compulsory for the entity to whom they signed the treaties. [14] This is a huge step in the establishment of the foundation of data protection. By perfecting data privacy laws, the possibility of leakage would reduce greatly, the risk of transferring data also decreases. Consequently, the Chinese government maintains its control over the data produced within the Chinese territory. Drafts issued in many specific areas concerning data surely made a sensation in China because the Chinese government shows the sign that China is moving toward a comprehensive data law period and the level of protection could be able to compare to the European Union's standard, meaning that data, in general, are safer and well protected by Chinse "shield".

Nevertheless, 2021 indeed is a big year for not only cybersecurity law but a turning point for Chinese legal history where piles of laws are implemented. Those laws greatly specified multiple unclear terms which were stated in Cybersecurity Law (2014). After invaliding the General Principle of Civil Law of the People's Republic of China, the recently issued Civil Code of the People's Republic of China maintains Article 127 which stated that "Where any laws provide for the protection of data and network virtual property, such laws shall apply." [15] It states that data of citizens are being protected by law. Additionally, it also specified that the personal data of a natural person is protected by law. [16] The term "natural person" is also defined. [17] Additionally, one constantly mentioned phrase "cybersecurity review" is also unspecified by the Chinese government until 2020 when the Measure of cybersecurity review became effective. Also, the term "critical information" remained undefined until the recently issued Critical Information Infrastructure Regulation. With the aim of maintaining data security and avoiding attacks, intrusion, and interruption and destruction of data[18], CII Regulation made a specification on the distinctive roles of each of the departments.[19]

Additionally, the Data Security Law (DSL) which was established in August of 2021 also reinforces the Chinese "shield" model. It is an important law because while it ensures domestic data security, it also made sure the safety of cross-border data transfer. Firstly, according to article 21 of DSL[20], China implemented the classification of data that corresponded to GDPR's data classification. Secondly, the security risk assessment is also needed to perform in order to transfer data abroad according to article 22 of DSL. China also strongly asserted article 26, namely, where any nation or region employs discriminatory, restrictive, or other similar measures against the PRC in terms of areas such as investment or trade-in data and technology for the exploitation and development of data, the P.R.C. may employ equal measures against that nation or region based on the actual circumstances, to firmly seize the sovereignty over data inside the territory of China. At the security level, greater protection is ensured by highly live of scrutiny, assessments and additional emergency mechanism. [21] At the

[13] Measures for Security Assessment of Cross-Border Data Transfer of Personal Information (For Public Comment) article 5 & 6.

[14] Personal Data Protection Law Article 38 (3). Full text see https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

[15] Civil Code of People's Republic of China.

[16] Id. art. 111

[17] Id. art.13

[18] CII art. 5

[19] CII art. 3& 4

[20] DSL art.21: The state is to establish a categorical and hierarchical system for data protection and carry out categorized and graded data protections based on the importance of the data in economic and social development as well as the extent of harm to national security, the public interest, or the lawful rights and interests of individuals or organizations that would be caused once the data is altered, destroyed, leaked, or illegally obtained or used. The national mechanism for coordinating data security work is to plan and coordinate relevant departments' drafting of catalogs of important data and strengthen protections of important data.

[21] DSL art.21

controlling level, Data Security Law allows cross-border data flow with sanctions from certain institutions. [22] Interestingly, DSL along with Article 4 of the International Criminal Judicial Assistance Law of the People's Republic of China, forms a Chinese version of "blocking statues" according to a Chinese scholar [33]. This response to the "long-arm" jurisdiction of the CLOUD Act, creates tension between two world power. At the same time, China can also adopt measures when it comes to the boycott of foreign companies which is a form of "long-arm" jurisdiction.[23] This protects domestic companies when competing with a foreign counterpart, making China have greater power in international competition. At the possession level, certain measures and procedures are needed to obtain data from Chinese institutions.

Furthermore, Personal Information Protection Law (PIPL) introduces detailed rules about cross-border data transfer. Primarily, a specified level of "security assessment" is required to transfer data abroad. Article 38 of PIPL stated that unless either having circumstances like "passing a safety assessment organized by the state internet information departments", "Having a professional body conduct personal information protection certification", having "contracts concluded with the overseas recipient parties" or retaining "other conditions provided for by laws, administrative regulations, or provisions"[24], no cross-boarder data transfer will happen. What's more, PIPL also established the role of "gatekeeper" [34] where the Chinese governments require "handlers" who "provide foundational internet platforms" to take responsibility to ensure that personal information is protected[25]. Didi case is a typical example of breaching this law where Didi has the potential to transfer data abroad even if it is in a position of "handler".

From the beginning of the internet era, Chinese strategy toward the internet and data shows signs of "shielding" and "isolation" by implementing a firewall to block foreign websites from "invading" [35]. The Chinese government blocks many the websites like YouTube and Instagram for the purpose of reducing exposure to western thought and reduce the risk of data extraction.

### *D. The current "Spear and Shield" With Didi Case Study*

With the prevalence of big data and the time when personal data are easily exposed, data sovereignty increasingly become a hotly debated topic among nations. Countries including China and the United States also started to take action. China mainly applied the "protectionist approach" while the United States utilized the "expansionist strategy". Coinciding with international lawfare, the case study of Didi's IPO could be characterized as an epitome of the "Spear and Shield" lawfare between China and the United States.

At the domestic level, the American government extracts data from foreign companies during their listing by implementing Sarbanes-Oxley Law (SOX) which stated that audits are required by the U.S. Securities and Exchange Commission for the process of publicizing corporates according to section 104 of the SOX. This was supplemented by recently established Holding Foreign Company Accountable[26]

In December 2020, U.S. Congress passed the Holding Foreign Companies Accountable Act (HFCAA), which was later signed by President Donald Trump. HFCAA provides additional requirements for the audit of foreign companies that are intended to be listed on the NYSE. To be specific, any corporate that failed to fulfill three years of PCAOB's audit would be delisted by U.S. Securities and Exchange Commission (SEC)[27]. Additionally, the audit data should be revealed by the U.S. registered accounting firms [36]. This is mostly because of the existing issue where the Chinese firms usually did not comply with Wall street audit rules. One famous example was that Luckin faked the audit data for IPO which resulted in a significant amount of fine [37]. Conversely, China also implemented Capital Market Law which few specifications were made. As a result, based on the Chinese Capital Market Law which authorizes the power to the Chinese government upon the Chinese firms who are listed outside of China. In addition to the Cybersecurity Law which emphasizes that the oversea firm couldn't extract data from the China mainland without the approval of the Chinese governmental institution, Chinese defensive weapon-"shield" is constructed. The conflicts in law potentially created a "Spear and Shield" lawfare where the United States expands data sovereignty outside of the geographic boundary to extract data from oversea corporate by the mean of domestic law and China strives for keeping the data sovereignty.

The logic behind Didi's incident is carried out by the mean of laws and regulations which came out recently and long before. It is the recently established cybersecurity measures that clash with the SEC's long-term frustration toward Chinese firms, and the lawfare was sparked. However, what exactly are those laws? And which U.S. law confronted Chinese laws? To begin with, Security Exchange Act is worth mentioning. Didi Chuxing is an "issuer" according to section 3 (8) of the Security Exchange Act which states that "the term 'issuer' means any person who issues or proposes to issue any security".[28] According, Didi could be defined as an issuer. As a "covered issuer", Didi is required to file an annual report until "that company is not an issuer."[29] The content of the audit is defined in section 10A(a)(1) which stated that illegal activity would be detected during the audit which means personal data could be investigated too.

However, not until the recently signed Holding Foreign Company Accountable Law, does the U.S. eventually make moves to deter Chinese firms through the mean of domestic laws. It is stated in Section 2(i)(2)(A) that "each covered issuer that, with respect to the preparation of the audit report on the financial statement of the covered issuer that is included in a report filed by the covered issuer, retains a registered public accounting firm that has a branch or office that is located in a foreign jurisdiction."[30]

This frustrated the Chinese government because auditing for Chinese companies is usually done by auditing firms based in China, meaning that the data is safely kept within

[22] Id. art.33
[23] Id. art. 24
[24] PIPL art. 38
[25] PIPL art. 58
[26] HFCAL section 2 (i)(2)(A)
[27] HFCAL Section 2(i)(2)(A)
[28] Security Exchange Act of 1934 section 3(c)(8)
[29] Id. section 13(a)(2)
[30] HFCAL Section 2(i)(2)(A)

Chinese territory and under the control of the Chinese government. Further demands were stated in Section 2(i)(3)(A) of HFCAL that "a covered issuer has 3 consecutive-inspection years, the Commission shall prohibit the securities of that covered issuer from being traded—on a national securities exchange or…" [31] , meaning that companies like Didi should comply the law immediately and handing auditing data of U.S standard in around 2024 [33]. Otherwise, it would be delisted. What's more, according to the Patriot Act, the government could access data that is stored in cloud servers of the U.S. providers [18]. However, there is a possibility of the audit firm utilizes those cloud servers, which indicates a risk that Chinese firms' audit data might be exposed to the U.S. government and it is legally justified. Actions including legalizing data acquisition and possible extraction of data from Chinese firms ensure the "long-arm jurisdiction", meaning that using the domestic law to regulate events happening overseas. In this case, those laws are used to expand t\U.S. data sovereignty over the Chinese firms and possibly data produced in China as a whole. The key debate is which authority truly has the right over the data produced by Didi.

Let's hear the Chinese version of the lawfare. To cope with the imposition of law from the U.S. government, the Chinese government implemented laws and measures which resemble a "shield" that aims to defend the data sovereignty from the intrusion of the "spear-like" legal strategy of the United States. Their main goal is to deter U.S. security regulators to access audit files of Chinese companies listed in the U.S. [3]. The governmental institution obtained the authority over the Chinese firms that are listed outside of China by the recently published Capital Market Law. To be specific, based on Act 2 of CML, Chinese firms who are listed outside of China are subjected to legal punishment if they disturb the domestic market order. As a result, the Chinese government has sovereignty over the Chinese firm's oversea exchange activities. Applying this law to Didi case where Didi has been suspected of data breach [38], Chinese data laws and policies should be emphasized.

The logic behind this data lawfare is mainly because of the nature of data. First, the data pool for auditing for Didi is massive and valuable, and Didi's data's depth is profound, meaning that those data are sensitive personal information[32] which could directly reflect the demographic, business distribution, population changes and much significant data [39]. As a result, the possible exposure of 377 million Chinese annual active drivers and 13 million annual active drivers' personal data was exposed to the governmental institutions in the U.S. would be disastrous. The accounting information includes cellphone numbers and real names along with the identification [40].

To summarize, the service produced by Didi belongs to the category of Critical Information Infrastructures, institutions that will produce significant data. This demonstrates that if the data leaking happened; the "critical information" would produce national security threats according to the definition from article 31 of Cybersecurity law. As a result, according to the Chinese government, Didi's listing poses a threat to "national security" because of the possible data breach based on Cyber Security Law and National Security Law [2]. According to article 35 of Cybersecurity Law, the Chinese government consequently announced that the cybersecurity review is needed for Didi in order to follow the guideline of Measures for Cybersecurity Review (2020). During this review, governmental departments would assess multiple areas, for instance, is there any "risk of important data being stolen, leaked, or harmed", and does "the supplier of the product or services' compliance with the Chinese law, administrative regulations, and departmental rules?" Laws like CSL and MCR certainly act as a defensive "shield" in this lawfare. As a consequence, Didi was being investigated by the Chinese Administration of Cybersecurity, followed by the removal of Didi from the app store and postponment of registration for new users [41]. This is among the first investigation after the Measure for Cybersecurity Review was first issued. In this investigation, China finally shows her "teeth" to the domestic companies that try to get listed abroad [42].

The lawfare was initiated by accumulated dissatisfaction between China and the U.S. For the United States, Wall Street was frustrated for years that Chinese corporate didn't follow the rule of submitting U.S. standard audit information even with the implementation of Holding Foreign Companies Accountable Act. However, China also feels uncomfortable with the U.S. approach of extracting massive valuable data from Chinese corporates. China is unlikely to allow data breaches in various forms.

## IV. Conclusion

This research proposes a 'Spear and shield framework' to help understand the nature of the current Data Sovereignty embodied in China-U.S. data legislation. By applying doctrinal, historical and comparative research, along with some international relations and political economy approaches, the research paper addresses the problem in a relatively comprehensive way. This research first introduced a theoretical framework of 'spear and shield' by introducing the background which initiate the topic. The paper then moves on to explain the doctrines and historical developments of these laws in China and the U.S., from the internet age to the data era. Finally, the research provides an analysis of the different data laws using the 'spear and shield framework and a deep analysis of the Didi case.

While the research lacks primary sources in terms of interviews with leading experts and speeches at a convention primarily because of my lack of access as a high school student. Luckily, by reading blogs from leading experts, consulting professors and guiding from a master from elite universities, I would be able to have a comprehensive understanding of this topic. However, interviews and more instructive opinions would be better for the development of the research paper.

Nevertheless, few significances of this research needed to be presented. Theoretically, the model of "spear and shield" could certainly be used in many other circumstances for any conflicts in legislation. Practically, this analysis can provide guidelines and introduction for Chinese corporations who wanted to go public in countries like the United States. More

[31] Id. section 2(i)(3)(A)

[32] PIPL art.28

importantly, by reviewing this research paper, the reader would produce new thoughts which would help them to form more questions that are worth investigating.

Finally, "lawfare" in terms of data sovereignty is just a fraction of the whole picture. If we look at the relationship between China and the U.S. from a political economy perspective, this research paper needs further explorations.

## Conflict of Interest

The authors declare no conflict of interest.

## Acknowledgment

I would like to thank everyone who provide me with support during the process of conducting the research, which include my parents and boyfriend.

## Reference

[1] Lawfare. (October 2019). About Lawfare: A brief history of the term and the site. *Hard National Security Choices*. [Online]. Available: https://www.lawfareblog.com/about-lawfare-brief-history-term-and-site

[2] Cyberspace Administration of China (CAC). (July 2021). Announcement of the Cyber Security Review Office on launching a cyber security review of "Didi Chuxing". [Online]. Available: http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm

[3] S. Yu. (July 2021). Didi caught as China and US battle over data. *Financial Times*. [Online]. Available: https://www.ft.com/content/00403ae5-7565-413e-907d-ad46549375ba.

[4] Big Data Analytics. IBM. (n. d.). [Online]. Available: https://www.ibm.com/analytics/hadoop/big-data-analytics

[5] Sovereignty. (June 2021). In Merriam-Webster.com. [Online]. Available: https://www.merriam-webster.com/dictionary/sovereignty

[6] Legal Information Institute. (August 2021). Sovereignty. legal information institute. [Online]. Available: https://www.law.cornell.edu/wex/sovereignty#:~:text=Sovereignty%20is%20a%20political%20concept,dominant%20power%20or%20supreme%20authority.&text=Sovereignty%20is%20essentially%20the%20power,power%20of%20others%20to%20interfere

[7] C. J. Dunlap, "Lawfare today: A perspective," *Yale J. Int'l Aff.*, vol. 3, pp. 146-154, Jan. 2008.

[8] Merriam-Webster.com. (June 2021). Spear. *Merriam-Webster.com*. [Online]. Available: https://www.merriam-webster.com/dictionary/spear

[9] Merriam-Webster.com. (October 2021). Shied. *Merriam-Webster.com*. [Online]. Available: https://www.merriam-webster.com/dictionary/shield

[10] J. Zittrain, "Law and technology the end of the generative internet," *Commun. ACM*, vol. 52, no. 1, pp. 18-20, Jan. 2009.

[11] J. R. Reidenberg, "Technology and Internet jurisdiction," *U. Penn. Law Rev.*, vol. 153, no. 6, pp. 1951-1974, Jun. 2005.

[12] J. Liu, "China's data localization," *Chin. J. Commun*., vol. 13, no. 1, pp. 84-103, Jun. 2020.

[13] Y. Wang, "Analysis on the jurisdiction of cyber data localization legislation," *J. Xi'an Jiaotong Univ. (Soc. Sci.)*, vol. 36, no. 1, pp. 54-61, Jan. 2016.

[14] U.S. Department of Justice. (2019). Promoting public safety, privacy, and the rule of law around the world: The purpose and impact of the cloud act. *U.S. Department of Justice*. [Online]. Available: https://www.justice.gov/opa/press-release/file/1153446/download

[15] J. Selby, "Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both?" *Int. J. Law Inf. Technol*., vol. 25, no. 3, pp. 213-232, July 2017.

[16] aosphere. (August 2021). Data privacy in the us: Insights from Aosphere. *Aosphere*. [Online]. Available: https://www.aosphere.com/aos/news-knowhow/data-privacy-in-the-us-insights-from-aosphere

[17] L. Cao, "Research on data rights in cyberspace," *Int. Observ*., vol. 1, pp. 53-58, 2013.

[18] A. C. Lakatos. (January 2012). The USA patriot act and the privacy of data stored in the cloud: Perspectives & events: Mayer brown. *Mayer Brown*. [Online]. Available: https://www.mayerbrown.com/en/perspectives-events/publications/2012/01/the-usa-patriot-act-and-the-privacy-of-data-stored

[19] G. Shen, "Great state to unite people: Data sovereignty and the national data strategy in a big data era," *Nanjing J. Soc. Sci*., vol. 6, pp. 113-127, 2014.

[20] D. Rushe. (January 2013). Google report reveals continued rise in us government requests for data. *The Guardian*. [Online]. Available: https://www.theguardian.com/technology/2013/jan/23/google-transparency-report-government-data-privacy

[21] T. Brewster. (March 2017). Now those privacy rules are gone, this is how isps will actually sell your personal data. *Forbes*. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2017/03/30/fcc-privacy-rules-how-isps-will-actually-sell-your-data/?sh=64f5babb21d1

[22] C. Cadwalladr and E. Graham-Harrison. (March 2018). Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach. [Online]. Available: The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[23] E. MacAskill, G. Dance, F. Cage, G. Chen, and N. Popovich. (November 2013). Nsa files decoded: Edward snowden's surveillance revelations explained. *The Guardian*. [Online]. Available: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[24] Court of Justice of the European Union. (2015). The court of justice declares that the commission's us safe harbour decision is invalid. *CVRIA*. [Online]. Available: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[25] U.S. Department of Commerce. (March 2021). Faqs – eu-u.S. Privacy shield program update. *Privacy Shield*. [Online]. Available: https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update

[26] S. Feng, "Data game and legal response in banning of tiktok," *Orient. Law*, no. 1, pp. 74-89, 2021.

[27] J. Daskal, "Microsoft ireland, the cloud act, and international lawmaking 2.0," *Stanf. L. Rev*. vol. 71, pp. 9-16, 2018.

[28] Y. Hong. ( April 2019). "The u.S. Quickly passed the cloud act to clarify its data sovereignty strategy," *Secrss*. [Online]. Available: https://www.secrss.com/articles/10196

[29] K. Klonick, "The new governors: The people, rules, and processes governing online speech," *Harv. Law Rev*., vol. 131, pp. 1598-1670, 2017.

[30] China Law Review. (August 2021). Promoting "one belt, one road" data cross-border flow in china. *Secrss*. [Online]. Available: https://www.secrss.com/articles/30719

[31] C. Girot. (2018). "Regulation of cross-border transfers of personal data in asia (softcover)." *Asian Business Law Institution*. [Online]. Available: https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia

[32] W. Hu, "The value orientation of cross-border data flow legislation and China's choice," *Soc. Sci*., vol. 4, pp. 95-102, 2018.

[33] Y. Hong. (July 2020). Understanding toward data security law-china's version of blocking decree. *Blog China*. [Online]. Available: https://net.blogchina.com/blog/article/997946511

[34] X. Ding. (August 2021). Expert interpretation of personal information protection law series. *Surging Government Affairs*. [Online]. Available: https://m.thepaper.cn/baijiahao_14219449

[35] European Parliament, "Geopolitical aspects of digital trade," 2020.

[36] T. Geron and S. Lu. (September 2021). Chinese companies listing in the u.S. Like didi face audit concerns. *Protocol*. [Online]. Available: https://www.protocol.com/sec-pcaob-china-audit

[37] E. Chung. (September 2021). Case study: Luckin coffee accounting fraud. *Sevenpillars Institute*. [Online]. Available: https://sevenpillarsinstitute.org/case-study-luckin-coffee-accounting-fraud/

[38] Nikkei Asia. (July 2021). China suspends didi app over data breaches days after us ipo. *Nikkei Asia*. [Online]. Available: https://asia.nikkei.com/Business/Companies/China-suspends-Didi-app-over-data-breaches-days-after-US-IPO

[39] N. Zhang. (2021). The "didi investigation" incident reflects the importance of data security responsibility. *China Urban and Rural Finance*. [Online]. Available: https://www.sohu.com/a/475769964_120032

[40] Y. Kubota and L. Lin. (July 2021). In the new china, didi's data becomes a problem. *The Wall Street Journal*. [Online]. Available: https://www.wsj.com/articles/in-the-new-china-didis-data-becomes-a-problem-11626606002

[41] H. Han, S. Chen, J. Liu, and H. Chen, "Data ethics, national security and overseas listing: A case study based on didi," *Financ Account Month*, vol. 15, pp. 13-23, 2021.

[42] M. Borak. (July 2021). What does didi's probe mean for the industry and china's tech giants? *South China Morning Post*. [Online].

Available: https://www.scmp.com/tech/big-tech/article/3139888/why-didis-cybersecurity-review-important-and-what-will-it-mean-ride