China Data Flows and Power in the Era of Chinese Big Tech

W. Gregory Voss, Emmanuel Pernot-Leplay

▶ **To cite this version:**

W. Gregory Voss, Emmanuel Pernot-Leplay. China Data Flows and Power in the Era of Chinese Big Tech. Northwestern Journal of International Law and Business, 2024, 44 (1), pp.1-68. hal-04513699

HAL Id: hal-04513699
https://hal.science/hal-04513699

Submitted on 20 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

Copyright 2024 by W. Gregory Voss and Emmanuel Pernot-Leplay
Vol. 44, No. 1
Northwestern Journal of International Law & Business

China Data Flows and Power in the Era of Chinese Big Tech

W. Gregory Voss[*] *and Emmanuel Pernot-Leplay*[**]

Abstract:

Personal data have great economic interest today and their possession and control are the object of geopolitics, leading to their regulation by means that vary dependent on the strategic objectives of the jurisdiction considered. This study fills a gap in the literature in this area by analyzing holistically the regulation of personal data flows both into and from China, the world's second largest economy. In doing so, it focuses on laws and regulations of three major power blocs: the United States, the European Union, and China, seen within the framework of geopolitics, and considering the rise of Chinese big tech.

First, this study analyzes ways that the United States—the champion of the free-flow of data that has helped feed the success of the Silicon Valley system—has in specific cases prevented data flows to China on grounds of individual data protection and national security. The danger of this approach and alternate protection through potential U.S. federal data privacy legislation are evoked. Second, the cross-border data flow restriction of the European Union's General Data Protection Regulation (GDPR) is studied in the context of data exports to China, including where the data transit via the United States prior to their transfer to China. Next, after review of the conditions for a European Commission adequacy determination and an examination of recent data privacy legislation in China, the authors provide a preliminary negative assessment of the potential for such a determination for China, where government access is an important part of the picture. Difficult points are highlighted for investigation by data exporters to China, when relying on EU transfer mechanisms, following the Schrems II jurisprudence.

Finally, recent Chinese regulations establishing requirements for the export of

[*] Associate Professor of Business Law, TBS Business School, Toulouse, France. This co-author holds a Juris Doctor from the University of Michigan Law School, a DESS Droit et systèmes d'information (now called Master 2 Droit du Numérique (Digital Law)) from Université Toulouse Capitole (France), and a BSFS from Georgetown University's School of Foreign Service, and may be reached at g.voss@tbs-education.fr.

[**] Principal, Data Privacy Specialist, Schneider Electric, Paris, France. This co-author holds a Ph. D. in comparative data protection law from Shanghai Jiao Tong University. Part of the underlying research for this article was carried out during a post-doctorate fellowship at Tilburg University, Tilburg Institute for Law, Technology, and Society (TILT). This co-author may be reached at pernot.emmanuel@gmail.com.

data are studied. In this exercise, light is shed on compliance requirements for companies under Chinese law, provisions of Chinese data transfer regulations that are similar to the those of the GDPR, and aspects that show China's own approach to restrictions on data transfers, such as an emphasis on national security protection. This study concludes with the observation that restrictions for data flows both into and out of China will continue and potentially be amplified, and economic actors will need to prepare themselves to navigate the relevant regulations examined in this study.

TABLE OF CONTENTS

I. INTRODUCTION

Personal data are a "powerful economic and political asset," benefiting those who control them.[1] Indeed, the concept of power is central to current analysis of personal data protection, sometimes referred to as "data privacy" or "privacy," and specifically to the regulation of data flows.[2] "Power" means many things, but one definition is "possession of control, authority, or influence over others."[3] Indeed, holding data, which have been described as "the chief source of power on the Internet," gives a kind of power: to understand, to read, and to act.[4] It can also lead to economic power, resulting from the innovation data allows.[5] Perhaps more to the point, according to an independent task force for the Council on Foreign Relations, data are "a source of geopolitical power and competition … seen as central to economic and national security."[6] Based on differing strategic aims discussed in this study, three major power blocs—the United States, the European Union, and China—have distinct forms of data privacy law regulation, providing fertile ground for comparative law study. Exports of personal data outside of one such jurisdiction may in certain circumstances generate concern, and thus provoke legislative or regulatory responses. In such context, this study focuses on restrictions to data flows to China from the United States and the European Union, and from China to the European Union, the United States, and other nations. In doing so, it seeks to provide a global viewpoint of the issues involved in this crucial area of law, and thus ease understanding.

In cases where there is regulatory divergence, such as in the area of data privacy law,[7] soft power, such as that of the "Brussels Effect," may be

---

[1] JEAN TIROLE, ECONOMICS FOR THE COMMON GOOD 401 (trans. Steven Rendall, 2017).

[2] *See, e.g.*, JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 5 (2019) ("Through their capacities to authorize, channel, and modulate information flows and behavior patterns, code and law *mediate* between truth and power."). *See also*, HENRY FARRELL & ABRAHAM L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY, 175–176 (2019) (Referring to the adoption of the European Union's General Data Protection Regulation: "This new willingness of the European Union to use its regulatory powers to shape international data flows is causing alarm among US commentators, and is likely to lead to new cross-national alliances, spurring further conflicts over privacy and power." (citation omitted)) [hereinafter OF PRIVACY AND POWER].

[3] *Power*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/power (last visited Dec. 19, 2022).

[4] *See* KIERON O'HARA & WENDY HALL, FOUR INTERNETS: DATA, GEOPOLITICS, AND THE GOVERNANCE OF CYBERSPACE 20 (2021).

[5] *See, e.g.*, Matthew J. Slaughter & David H. McCormick, *Data Is Power: Washington Needs to Craft New Rules for the Digital Age*, FOREIGN AFF., May/June 2021, at 54, 56–57.

[6] Council on Foreign Relations, *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet* 3 (Independent Task Force Report No. 80, 2022), https://www.cfr.org/report/confronting-reality-in-cyberspace [hereinafter *Confronting Reality in Cyberspace*].

[7] W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485, 489–93 (2020) [hereinafter *Cross-Border Data Flows*].

exercised indirectly by encouraging multinational actors to adopt the higher data protection standards of the European Union worldwide, for example.[8] Furthermore, such divergence in standards may be due in part to the economic power that control of personal data allows,[9] and may be the motor behind "rival standards" where the proponents of each of the different standards will aim to weaken competing ones.[10] Indeed, China goes outside of the traditional U.S.-based internet governance structures to work through the United Nations and the International Telecommunication Union, instead, on issues of data governance to further cyber sovereignty.[11] China seeks to be a "norm entrepreneur" in this area and sees data as a "national strategic resource."[12] China's emphasis on national security, sovereignty, and economic development differs from the European Union's focus on fundamental rights,[13] although each may be described as related to a certain strategic view,[14] leading to a form of power.

In a manner like the strategic aims of their European Union and Chinese counterparts, the U.S. approach, involving lack of effective data privacy law and a self-regulation focus, may have allowed for the development of the U.S. tech giants,[15] providing economic power, as well as access to data, for antiterrorist and law enforcement purposes. However, U.S. influence on digital trade governance worldwide may be hampered by its distaste for multilateral trade agreements.[16] Also, the lack of European Union-style data

---

[8] *Anu Bradford*, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 140–141 (2020) [hereinafter THE BRUSSELS EFFECT]. *See also* Oskar Josef Gstrein & Andrej Janko Zwitter, *Extraterritorial Application of the GDPR: Promoting European Values or Power?*, 10(3) INTERNET POL'Y REV. (2021). (considering the "Brussels Effect" as "a power-based approach, since it combines elements of political and economic capability to determine societal and normative developments in a particular area.").

[9] THE BRUSSELS EFFECT, *supra* note 8, at 141.

[10] *See* DANIEL W. DREZNER, ALL POLITICS IS GLOBAL: EXPLAINING INTERNATIONAL REGULATORY REGIMES 79, 103–106 (2019).

[11] *See Confronting Reality in Cyberspace*, *supra* note 6, at 19–20 ("Beijing and Moscow are collaborating to reshape the global internet and reduce U.S. influence. . . . The two countries have also promoted cyber sovereignty through the United Nations, International Telecommunication Union, Shanghai Cooperation Organization, and the BRICS group (Brazil, Russia, India, China, and South Africa)." (citation omitted)).

[12] *See* Xuechen Chen & Xinchchu Gao, *Comparing the EU's and China's Approaches in Data Governance*, *in* UNDERSTANDING THE EU AS A GOOD GLOBAL ACTOR: AMBITIONS, VALUES AND METRICS 209, 218 (Elaine Fahey & Isabella Mancini, eds., 2022).

[13] *See id*. at 219.

[14] *See, e.g.*, *Cross-Border Data Flows*, *supra* note 7, at 489–93 (specifically discussing strategic goals of China, the European Union, and the United State in relation to data privacy).

[15] *See, e.g.*, Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 667 (2014) (referring to Silicon Valley and U.S. law, Chander wrote: "Because the businesses are innovating new relationships between users and information, the risk to privacy in this process of experimentation is especially high. A liberal privacy regime thus proves conducive to this kind of trial-and-error method for innovation, allowing companies to base their offerings not on legal constraints but on market reaction.").

[16] *See Confronting Reality in Cyberspace*, *supra* note 6, at 22 ("The U.S. withdrawal from

privacy law may prejudice U.S. efforts to protect individual privacy and, relatedly as will be shown in Part I, national security. Truly, the world has entered a phase where internet governance has become multipolar,[17] and geopolitics plays a role in how the fundamental right to data protection (to use the European concept and terminology) is protected around the globe,[18] with evident tensions between the United States and China in the background.[19] At stake are rights, values, and strategy, but also an estimated almost $3 trillion in cross-border data flows and digital services.[20]

In such an environment, where national strategic goals are at play, it is easy to see why various jurisdictions choose to regulate cross-border data flows. However, forms of such regulations have existed since the 1980s and earlier, based on fears of the impact of such flows on privacy protection.[21] Furthermore, these regulations, in their most recent versions (here, in the European Union and China), rather than being played out on some virtual global chessboard, have impact on individual rights and how firms carry out their business. They help constitute what has now become a highly regulated area of business activity.

The United Nations Conference on Trade and Development (UNCTAD) provides a taxonomy, mapping regulations on cross-border data flows divided into three approaches and five categories. These are: the restrictive or guarded approach, which is made up of the strict data

---

the Trans-Pacific Partnership and continued aversion to multilateral trade agreements severely limit its ability to shape the rules guiding digital trade." Or, more succinctly, "The United States has taken itself out of the game on digital trade.").

[17] *See, e.g.*, Eric Geller, *China, EU Seize Control of the World's Cyber Agenda*, POLITICO (July 22, 2018 07:01 AM EDT, updated July 24, 2018 09:53AM EDT), https://www.politico.com/story/2018/07/22/china-europeglobal-cyber-agenda-us-internet-735083 ("The United States is losing ground as the internet's standard-bearer in the face of aggressive European privacy standards and China's draconian vision for a tightly controlled Web." And "[t]he result; Beijing and Brussels are effectively writing the rules that may determine the future of the internet.").

[18] *See* Monique Mann & Angela Daly, *Geopolitics, Jurisdiction and Surveillance*, 9(3) INTERNET POL'Y REV.1, 2–4 (2020).

[19] As an example, in February 2023 the United States shot down an alleged Chinese spy balloon, reflecting this tension. *See* Yu Jie, *The Spy Balloon Saga Says Far More About Biden's Political Weakness than China's Strength*, GUARDIAN (Feb. 8, 2023, 14:35 GMT), https://www.theguardian.com/commentisfree/2023/feb/08/spy-balloon-joe-biden-china-us-republicans (in connection with the balloon affair, the author of an opinion piece characterizes the bilateral relationship as one of "volatility and competition," and claims that, "The benefits of many fundamental elements of the US-China relationship, such as trade and investment, have been rapidly diminishing as a result of Chinese companies' increasing commercial competitiveness and generous subsidies from Beijing. In military and technology terms, the two countries have become ultra-competitive, rather than needing to work together.").

[20] *See Confronting Reality in Cyberspace*, *supra* note 6, at 20.

[21] Fears of "data protectionism" existed back then, but so was there a recognition that such flows could have a negative effect on privacy, circumventing protective legislation in one jurisdiction by storing data in a less protective country. *See* Michael D. Kirby, *Transborder Data Flows and the Basic Rules of Data Privacy*, 16 STAN. J. INT'L L. 27 (1980).

localization and partial data localization categories; the prescriptive approach which is constituted by the conditional transfer; hard and the conditional transfer; intermediate/soft categories; and the light-touch approach, which is made up of the free flow of data category.[22] In UNCTAD's taxonomy, China figures in the restrictive or guarded approach, the European Union in the prescriptive approach, and the United States in the light-touch approach column[23] thus covering the full spectrum. While this taxonomy is helpful as a starting place, more must be done to flesh out the distinct specificities of each of the power blocs' regulations in this regard, together with their nuances and their paradoxes.

Much academic literature has already analyzed legal issues involving the transfer of personal data specifically from the European Union to the United States.[24] There are several possible explanations for this: first, the two blocs are each other's largest trading partner, which might explain the focus.[25] Secondly, U.S. big tech companies have dominated the data economy for many years and have correspondingly attracted much attention.[26] Furthermore, the Edward Snowden revelations regarding the

---

[22] *See* U.N. Conference on Trade and Development, *Digital Economy Report 2021,* Table V. 3, at 137, U.N. Doc. UNCTAD/DER/2021 [hereinafter UNCTAD].

[23] *Id*. at 137.

[24] *See, e.g.*, Griffin Drake, *Navigating the Atlantic: Understanding EU Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163 (2017); Fumiko Hirasawa, *Approaches to Realizing Legal Interoperability Between the Data Privacy Regimes of the European Union and the United States*, 28 COLUM. J. EUR. L. 282 (2022); Emily Linn, *A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement*, 50 VAND. J. TRANSNAT'L L. 1311 (2017); Xavier Tracol, *"Schrems II": The return of the Privacy Shield*, 39 COMPUTER L. & SEC. REV. Article 105409 (2020) [hereinafter Tracol]; Danijela Vrbljanac, *Personal Data Transfer to Third Countries – Disrupting the Even Flow?*, 4 ATHENS J. L. 337 (2018); and W. Gregory Voss, *Transatlantic Data Transfer Compliance*, 28 B.U. J. SCI. & TECH. L. 158 (2022) [hereinafter *Transatlantic Data Transfer Compliance*]. *See also*, ELAINE FAHEY, THE EU AS A GLOBAL DIGITAL ACTOR: INSTITUTIONALISING GLOBAL DATA PROTECTION, TRADE, AND CYBERSECURITY 183 (2022) ("It is possible that excessive amounts of attention are focused on transatlantic transfers, rather than EU-Asian transfers.") [hereinafter THE EU AS A GLOBAL DIGITAL ACTOR].

[25] DANIEL S. HAMILTON & JOSEPH P. QUINLAN, THE TRANSATLANTIC ECONOMY 2021: ANNUAL SURVEY OF JOBS, TRADE AND INVESTMENT BETWEEN THE UNITED STATES AND EUROPE 17 (2021), https://www.uschamber.com/assets/archived/images/transatlanticeconomy2021_fullreport_lr.pdf. Another author, speaking of the European Union and the United States, comments, "While China is less connected with the other two systems in terms of cross-border data flow, the US system seems to be the most embroiled in the struggle for data protection online …." Oreste Pollicino, *Data Protection and Freedom of Expression Beyond EU Borders: EU Judicial Perspectives*, *in* DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES ON EXTRATERRITORIALITY AND SOVEREIGNTY 81, 84 (Federico Fabbrini, Edoard Celeste & John Quinn, eds., 2021) (citation omitted).

[26] *See, e.g*., Maria Helen Murphy, *Assessing the Implications of* Schrems II *for EU-US Data Flow*, 71 INT'L & COMPAR. L.Q. 245, 246 (2022) https://doi.org/10.1017/S0020589321000348 ("Indeed, the significance of the EU-US data transfer relationship is unparalleled, in large part due to the dominance of US technology companies and the size of the EU consumer market.").

mass surveillance of data by U.S. intelligence agencies and the cooperation of U.S. big tech with them[27] has created concern and mistrust.[28]

Yet, Chinese websites[29] and applications (apps)[30] have grown popular worldwide, too, leading to what this study describes as a dawning era of Chinese big tech. China has become the second largest digital economy in the world, driven in part by data, and is growing.[31] Chinese firms Tencent and Alibaba have joined the club of the world's largest digital platforms as measured by market capitalization.[32] Among the fifteen top social networks by number of users in January 2023 are six Chinese networks: WeChat (fifth), TikTok (sixth), Douyin (eighth), Kuaishou (eleventh), Sina Weibo (twelfth), and QQ (thirteenth).[33] Part of the growth of Chinese big tech firms

---

[27] Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; *see also* Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[28] *See, e.g.*, Alan Travis, *Snowden Leak: Governments' Hostile Reaction Fuelled Public's Distrust of Spies*, GUARDIAN (June 15, 2015), https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies.

[29] *See, e.g.*, Claudia Biancotti, *The Growing Popularity of Chinese Social Media Outside China Poses New Risks in the West*, PETERSON INST. FOR INT'L ECON. (PIIE) (Jan. 11, 2019 8:00 AM), https://www.piie.com/blogs/china-economic-watch/growing-popularity-chinese-social-media-outside-china-poses-new-risks (specifically detailing the "rise of TikTok"). In 2019, fifteen of the top one hundred websites in the world were from China based on monthly visits, With one of them—Baidu.com—reaching fourth place. Nick Routley, Ranking the Top 100 Websites in the World, VISUAL CAPITALIST (Aug. 7, 2019), https://www.visualcapitalist.com/ranking-the-top-100-websites-in-the-world/ (cautioning that, "Brands that extend across platforms or serve the majority of their users through an app will not necessarily rank well on this list. As a result, you'll notice the absence of companies like WeChat and Snapchat.").

[30] John Koetsier, *Top Apps Of 2022 By Installs, Spend, And Active Users: Report*, FORBES (Mar. 23, 2022 07:32 PM), https://www.forbes.com/sites/johnkoetsier/2022/03/23/top-apps-of-2022-by-installs-spend-and-active-users-report/ (showing TikTok as the global app having the second highest number of downloads worldwide in the first quarter of 2022, being the highest for consumer spending during the same period (Tencent Video was sixth, iQiYi—a Chinese video publishing app—was ninth, and QQ Music—a Chinese freemium music streaming service owned by Tencent Music, a Tencent/Spotify joint venture, was tenth), and fifth for monthly active users during the same period).

[31] Joshua P. Meltzer, *China's Digital Services Trade and Data Governance: How Should the United States Respond*?, BROOKINGS (Oct. 2020), https://www.brookings.edu/articles/chinas-digital-services-trade-and-data-governance-how-should-the-united-states-respond/ (China's digital economy second only to the United States' digital economy).

[32] UNCTAD, *supra* note 22, at xv–xvi. *See also* Paul Mozur, *The World's Biggest Tech Companies Are No Longer Just American*, N.Y. TIMES (Aug. 17, 2017), https://nyti.ms/2vGaRq2 ("The Alibaba Group and Tencent Holdings, Chinese companies that dominate their home market, have rocketed this year to become global investor darlings. They are now among the most highly valued public companies, each of them twice as valuable as tech stalwarts such as Intel, Cisco and IBM.").

[33] *Most Popular Social Networks Worldwide as of January 2023, Ranked by Number of*

may be due to actions of the Chinese government, with which they are said to have a "symbiotic" relationship.[34] Furthermore, NikkeiAsia reported that in 2019, China (including Hong Kong) then accounted for 23% of cross-border data flows, nearly twice the U.S. share of 12%, placing China/Hong Kong in the top position; at the same time, U.S. share of data flows in and out of China had dropped to 25%.[35] Importer countries for cross-border data transmission from China (including Hong Kong), in order of their percentage share, were the United States, followed by Japan, and then the United Kingdom, France, and Germany, grouped together.[36] In this mix, big tech companies, such as the Chinese companies Alibaba, TikTok, and Tencent, are playing an important role in shaping geopolitics.[37]

However, the success of international markets has caused wide debate, involving issues of privacy, national security, and "technological and economic hegemony,"[38] which is another aspect of power. Furthermore, Chinese companies and data flows to China have begun to come on the radar of European data regulators. For example, in 2021, the Netherlands' data regulator fined Chinese company TikTok €750,000 for privacy violations involving children,[39] and in 2021, Ireland's data regulator announced that it had launched two investigations of that same company, for data protection compliance involving children's personal data and transfers of data to

Monthly Active Users (in Millions), STATISTA, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (last visited May 27, 2023).

[34] Part of Chinese big tech firm growth may be attributable to actions of the Chinese government: "The Chinese government has strategically cultivated its national technology champions, in part by banning foreign competitors and using policy incentives to favor domestic firms, which has resulted in a symbiotic partnership between the Chinese government and its commercial internet firms." Natasha Tusikov, *Internet Platforms Weaponizing Choke Points*, *in* THE USES AND ABUSES OF WEAPONIZED INTERDEPENDENCE 133, 144 (Daniel W. Drezner, Henry Farrell & Abraham L. Newman, eds., 2021).

[35] Toru Tsunashima, *China Rises as World's Data Superpower as Internet Fractures*, NIKKEIASIA (Nov. 25, 2020 20:30), https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures (this article cites the International Telecommunications Union (ITU) and U.S. research firm TeleGeography as sources for their data, but does not specify whether the statistics include both personal and non-personal data. As it is difficult to separate out and measure personal data flows, these figures are typically aggregated.).

[36] *Id.*

[37] Ian Bremmer, *The Technopolar Moment: How Digital Powers Will Reshape the Global Order*, FOREIGN AFF. 112, 113 (Nov./Dec. 2021).

[38] Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's Digital Silk Road as Transnational Data Governance*, 54 N.Y.U. J. INT'L L. & POL. 1, 5–6 (2021) (referring to debate in reaction to the entry of WeChat and TikTok, in addition to Chinese networking equipment providers, in the U.S., U.K., and Japanese market) (citation omitted) [hereinafter *The Beijing Effect*].

[39] *Dutch DPA: TikTok Fined for Violating Children's Privacy*, EUR. DATA PROT. BD. (July 22, 2021), https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en.

China.[40] Also, in 2021, Norway's data regulator fined Norwegian company Ferde AS approximately €500,000 for having transferred personal data to China without a legal basis and without having implemented a data transfer mechanism.[41] Next, in late 2022, France's data regulator fined TikTok €5 million under a part of the French Data Protection Act that implements the ePrivacy Directive, as users of the TikTok website could not as easily refuse cookies and were not clearly informed about the purposes of different cookies.[42] Finally, although no longer in the European Union, the United Kingdom, which has similar data protection legislation to that bloc, fined TikTok £12.7 million in April 2023 for failing to use children's data lawfully.[43]

More signs appear to indicate a new European focus on data protection involving China. First, the Irish data regulator's investigation of TikTok's data protection compliance involving children's personal data, announced in 2021, led to a reprimand, an order to bring its data processing into compliance with the GDPR within three months, and an administrative fine, in the sizable amount of €345 million, on September 1, 2023.[44] Next, at the 10th EU-China High-Level Economic and Trade Dialogue held on September 25, 2023, concerns about cross-border data flows were reportedly raised by the European Union.[45]

Moreover, in this context, in a dawning era when Chinese big tech firms are becoming larger and more important economically, some work should be done on the issue of data transfers in and out of China, too. While academic

---

[40] *DPC Launches Two Inquiries into TikTok Concerning Compliance with GDPR Requirements Relating to the Processing of Childrens' Personal Data and Transfers of Data to China* DATA PROT. COMM'N (Sept. 14, 2021), https://www.dataprotection.ie/en/news-media/latest-news/dpc-launches-two-inquiries-tiktok-concerning-compliance-gdpr-requirements-relating-processing.

[41] *Transatlantic Data Transfer Compliance*, *supra* note 24, at 203–204. Data transfer mechanisms are discussed *infra* Part III. C.

[42] *Cookies: The CNIL Fines TIKTOK 5 Million Euros*, CNIL (Jan. 12, 2023). https://www.cnil.fr/en/cookies-cnil-fines-tiktok-5-million-euros. The ePrivacy Directive, which applies to the telecommunications sector and was amended in 2009, places requirements for prior informed consent for the placement of cookies on user devices in the European Union. *See* W. Gregory Voss, *First the GDPR, Now the Proposed ePrivacy Regulation*, 21 J. INTERNET L. 3 (July 2017).

[43] *ICO Fines TikTok £12.7 Million for Misusing Children's Data*, ICO (Apr. 4, 2023), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/.

[44] *Irish Data Protection Commission Announces €345 Million Fine of TikTok*, DATA PROT. COMM'N (Sept. 15, 2023), https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.

[45] Ulrich Jochheim, *At a Glance: Plenary – October 1, 2023: EU-China Trade Relations*, EUR. PARLIAMENT RSCH. SERV. (EPRS) (Sept. 2023), https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/753952/EPRS_ATA(2023)753952_EN.pdf; *see also EU-China Trade Talks Fail to Yield Results*, ECON. INTEL. (EIU) (Oct. 4, 2023), https://www.eiu.com/n/eu-china-trade-talks-fail-to-yield-results/.

articles have compared Chinese data law to European data protection law and U.S. privacy law,[46] the authors believe that this study is one of the first—if not *the* first—to focus on regulation of personal data transfers both into and out of China in a holistic way from a data protection perspective, and thus contributes to the literature. Perhaps this focus on China will also not displease some in the United States, who saw the EU-U.S. Privacy Shield framework, used for data flows from Europe to the United States, invalidated by the Court of Justice of the European Union (CJEU) in 2020 in its *Schrems II* decision.[47]

A year prior to that decision, a scholar selected by litigant Facebook as an expert on U.S. law in the Irish proceedings leading up to the referral to the CJEU in the *Schrems II* case[48] suggested that cutting off data flows to the United States should be accompanied by cutting off flows from the European Union to China and other states that allow government access to personal data without EU-level protections.[49] Already in 2013, Christopher Kuner had raised the specter of Chinese authorities compelling service providers to reveal data.[50]

Given the differences in legal systems and cultures and the importance of the issue for geopolitical and economic power, this study does not foresee any great move towards harmonization of data protection laws in the three blocs that it analyzes. Those differences include the neoliberalist policy of the United States and the pre-eminent position that the right to freedom of expression holds, and the fundamental rights status of the right to data protection in the European Union, which is not duplicated on the other side

---

[46] *See, e.g.*, Igor Calzada, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, 2022 SMART CITIES 1129 (2022); Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.*, 8 PENN ST. J.L. & INT'L AFF. 49 (2020) [hereinafter Pernot-Leplay]; and Philip Andreas Weber, Nan Zhang & Haiming Wu, *A Comparative Analysis of Personal Data Protection Regulations Between the EU and China*, 20 ELEC. COM. RSCH. 565 (2020).

[47] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximilian Schrems, ECLI:EU:C:2020:559 (July 16, 2020) [hereinafter *Schrems II*].

[48] *Professor Peter Swire Testimony in Irish High Court Case*, ALSTON & BIRD, https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony, (last visited Dec. 24, 2022).

[49] Peter Swire, *The US, China, and Case 311/18 on Standard Contractual Clauses*, EUROPEAN LAW BLOG (July 15, 2019), https://europeanlawblog.eu/2019/07/15/the-us-china-and-case-311-18-on-standard-contractual-clauses/. A similar point of view was taken more recently in an article by Hoffman. *See* David A. Hoffman, *Schrems II and TikTok: Two Sides of the Same Coin*, 22 N.C. J.L. & TECH. 573, 610–11 (2021) ("Therefore, the Court's Schrems decisions should not just call into question transfers of personal data from the EU to the United States, but also transfers to countries that have robust surveillance practices, but even less transparency, access to tribunals, or legally enforceable privacy protections. The list of countries should include … China.") [hereinafter Hoffman].

[50] CHRISTOPHER KUNER, Transborder Data Flows and Data Privacy Law 114 (2013) [hereinafter KUNER].

of the Atlantic.[51] Looking eastward, the priority that China places on national security, the relevant lack of emphasis it assigns to individual rights, and the low level of importance placed on privacy, mean that it is unlikely to harmonize its data protection regime with that of, notably, the European Union.[52] As Part I will show, the real unknown is how much the United States will drift toward, in part, each of the two other systems, with the U.S. concern for national security and the possible help that EU-style data transfer restrictions might allow it. Of course, the general context for this study is geopolitics, which has a great impact on business, and perhaps all the more so because of tensions between the United States and China.[53] Nonetheless, it is an underlying thesis of this study that personal data flows in and out of China are, and will continue to be, subject to limitations whether through legislation, concern for security and economic sovereignty made concrete by regulatory action, or by practice, and that this will negatively influence trade. However, it may also fulfill geopolitical goals.

The organization of this study after this introduction (Part I) is as follows: Part II starts with flows from the liberal United States, which has all the same employed arguments about national security and privacy to restrict certain flows to China in specific cases. Second, Part III continues with the European Union and its landmark data privacy legislation—the General Data Protection Regulation (GDPR)[54]—which provides for restrictions on certain personal data exports out of that bloc. Importation of such data by China is studied in that light. Third, Part IV analyzes recent Chinese law, including the important Personal Information Protection Law. Next, Chinese data transfer restrictions are detailed in Part V, and studied in the context of the possibility of an adequacy decision by the European Commission (Commission). This analysis should also prove helpful for firms conducting a transfer impact assessment for data exports to China. Finally, Part VI makes concluding remarks.

---

[51] W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 431–452 (2019) [hereinafter *Obstacles to Transatlantic Harmonization*] (positing differing constitutional legal culture, neoliberalism, and lobbying as obstacles to U.S. harmonization with EU data privacy law).

[52] *See, e.g.*, Li Yang & Min Yan, *The Conceptual Barrier to Comparative Study and International Harmonization of Data Privacy Law*, 51 H.K. L.J. 917, 937–40 (2021).

[53] *See, e.g.*, Michael A. Witt, *China's Challenge: Geopolitics, De-Globalization, and the Future of Chinese Business*, 15 MGMT. & ORG. REV. 687 (2019).

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

II. UNITED STATES TO CHINA DATA FLOWS

China is the largest goods trading partner of the United States.[55] As such, the trade relationship between the two countries is an important one. It leads to complex transnational supply chains, where an Apple iPhone may be "Designed in California. Assembled in China."[56] Data, which have been described as "the new oil," play a growing role in manufacturing,[57] and data flows are now considered crucial to trade,[58] although different from goods or services trade.[59] However, competition for power between the United States and China is causing tension in supply chains and triggering the imposition of controls on data flows,[60] which influence this study's analysis of data flows from the United States to China.

Part II starts by introducing the U.S. policy on data flows in its first section. The second section discusses two cases involving then Chinese-controlled Grindr and the Chinese company TikTok as exceptions to the rule. Then, the third section briefly considers the possible impact of proposed data privacy legislation in this context. Next, the fourth section highlights certain practices of Chinese companies dealing in the United States, prior to concluding in the fifth section. One additional subject—EU personal data that transits through the United States and then is subject to a transfer from the United States to China—will be covered in Part III.

---

[55] *The People's Republic of China: U.S.-China Trade Facts*, OFF. OF THE U.S. TRADE REPRESENTATIVE (last visited Feb. 5, 2023), https://ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china [hereinafter U.S.-China Trade Facts].

[56] *See, e.g.*, OF PRIVACY AND POWER, *supra* note 2, at 23.

[57] *See, e.g.*, Yan Xiao & Donnie Dong, *What Do China's Data Export Regulations Mean for Its Trade Competitiveness?*, WORLD ECON. F. (Nov. 30, 2022), https://www.weforum.org/agenda/2022/11/china-data-export-regulations-threaten-trade-competitiveness/.

[58] The OECD highlights the link between data and trade:

> Underpinning digital trade is the movement of data. Data is not only a means of production, it is also an asset that can itself be traded, and a means through which GVCs are organised and services delivered. It also underpins physical trade less directly by enabling implementation of trade facilitation. Data is also at the core of new and rapidly growing service supply models such as cloud computing, the Internet of Things (IoT), and additive manufacturing.

Digital Trade: The Impact of Digitalisation on Trade, OECD, https://www.oecd.org/trade/topics/digital-trade/ (last visited Jan. 29, 2023) (GVCs refers to global value chains).

[59] Susan Ariel Aronson, *Data Is Different, Why the World Needs a New Approach to Governing Cross-Border Data Flows*, 197 CTR. INT'L GOVERNANCE INNOVATION 1, 4–5 (2018) (describing some of the unique features of trade in data, including its fluidity, difficult-to-locate nature, lack of fit for a traditional definition of "trade," and so on).

[60] *Confronting Reality in Cyberspace*, supra note 6, at 8 ("The international competition for power is accelerating the fragmentation of technology spheres. Policymakers in the United States and China worry about intelligence activities introducing backdoors in software and hardware, interdicting products along the supply chain, and using both legal and extralegal means to access data held by technology firms. As a result, both countries have recently introduced new rules and measures designed to secure supply chains, exclude foreign suppliers and products, *and control the flow of data*." (emphasis added)).

A. INTRODUCTION TO U.S. POLICY ON DATA FLOWS

The United States has sectoral federal legislation with respect to certain financial,[61] health,[62] and children's data,[63] for example, but no comprehensive federal data privacy legislation.[64] Several factors have led to this result, including a laissez-faire approach that favors self-regulation, instead.[65] Consistent with such approach, the United States has traditionally opposed cross-border data flow restrictions,[66] considering them inappropriate.[67] At least in part, this position relates to power—economic power, and military power: in the mid-1970s, companies sought data for global market expansion, and the military for surveillance.[68] In the 1980s the United States was seen as "the world leader in information technology," with lots to lose because of limitations on transborder data flows.[69] To support open data flows, digital policy objectives of U.S. trade negotiators include ensuring against limitations being placed on data flows.[70] Clearly stated, the

---

[61] Gramm-Leach-Bliley Act (Financial Modernization Act of 1999), 15 U.S.C. §§ 6801–6809, and Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.

[62] Health Information and Portability Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29 & 42 U.S.C.).

[63] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

[64] *See, e.g.*, Jordan L. Fischer, *The Challenges and Opportunities for a US Federal Privacy Law*, *in* DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES ON EXTRATERRITORIALITY AND SOVEREIGNTY 27, 28 (Federico Fabbrini, Edoardo Celeste & John Quinn, eds., 2021) ("… there is no express individual right to privacy in the US nor is there any general privacy protecting legislation to date." (citations omitted)).

[65] *See, e.g.*, Lilian Edwards, *Reconstructing Consumer Privacy Protection On-line: A Modest Proposal*, 18 INT'L REV. L. COMPUTS. & TECH. 313, 316 (2004).

[66] *See, e.g.*, KUNER, *supra* note 50, at 115; *see also* David McCabe & Adam Satariano, *The Era of Borderless Data Is Ending*, N.Y. TIMES (May 23, 2022), https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html ("While the United States supports a free, unregulated approach that lets data zip between democratic nations unhindered . . . .").

[67] Briseida Sofia Jiménez-Gómez, *Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute*, 19 SANTA CLARA J. INT'L L. 1, 8 (2021).

[68] SUSANNA MONSEAU, LAW, TECHNOLOGY, AND BUSINESS: THE 21ST CENTURY CORPORATION AND THE FUTURE OF WORK 223 (2017) ("In the mid-1970s, American companies and the U.S. military started to amass large digital databases. U.S. companies wanted data for worldwide market expansion. The military was interested in the possibility of using digital data for surveillance purposes.").

[69] Garry S. Grossman, *Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations*, 4 NW. J. INT'L. L. & BUS. 1, 4–5 (1982); *see also* Dorine R. Seidman, *Transborder Data Flow: Regulation of International Information Flow and the Brazilian Example*, 1 J.L. & TECH. 31, 34–35 (1986) ("For the United States, any restrictions on the free flow of information would also hamper trade in services. The United States is presently the number one exporter of services in the world, generating close to $60 billion in revenue in 1980." (Citations omitted)).

[70] Kristin Archick & Rachel F. Fefer, *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917 CONG. RSCH. SERV. 5–6 (2021) ("In passing Trade Promotion Authority (TPA), Congress specified digital trade policy objectives for U.S. trade negotiations including to "ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or

United States does not place general restrictions on personal data exports based on data privacy.[71] However, U.S. policy established prior to the rise of Chinese big tech is worthy of review in light of changed circumstances.

B. SPECIFIC CASES: THE EXCEPTIONS

While U.S. policy is to allow for the free flow of data, and, indeed, to require it through free trade agreements, there are specific cases when it seeks to limit such free flow. These cases are the exception and represent exercise of government power based on grounds of national security and privacy of individuals. To illustrate this apparent paradox in a context where the United States itself has come under criticism from Europe for "national security surveillance,"[72] this study will briefly investigate two such exceptions involving a company that was Chinese-controlled at the time, and a Chinese company: respectively, Grindr and TikTok, the latter of which can now boast a total 150 million U.S. users.[73]

1. Grindr

While not the first case of the use of national security grounds to act against a Chinese company, the Grindr case is notable for its basis in protecting the data privacy of U.S. individuals. Prior to the Grindr case, Chinese telecommunications equipment provider Huawei was subject to various U.S. actions, including certain related to alleged espionage; intellectual property infringements; and being a threat to national security, in part related to the possible access to corporate data that it might allow the Chinese government.[74] However, the Grindr case more clearly involves

processing of data," while allowing exceptions for legitimate policy objectives that are nondiscriminatory and promote an open market environment." (Citation omitted)).

[71] *See, e.g.*, LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 110 (2014) ("… US legislation refrains from imposing privacy-related restrictions on export of personal data to other countries."). *See also* Svetlana Yakovleva, *The EU's Trade Policy on Cross-Border Data Flows in the Global Landscape: Navigating the Thin Line Between Liberalizing Digital Trade, 'Digital Sovereignty' and Multilateralism*, *in* UNDERSTANDING THE EU AS A GOOD GLOBAL ACTOR: AMBITIONS, VALUES AND METRICS 192, 196 (Elaine Fahey & Isabella Mancini, eds., 2022) ("Unlike the EU GDPR, US law does not restrict transfers of personal data outside the US. It has indeed been squarely argued that the US kept its privacy protection strategically low to promote digital commerce." (citation omitted)) [hereinafter Yakovleva].

[72] Kristina Irion, Margot E. Kaminski & Svetlana Yakoleva, *Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law*, U. CHI. L. REV. ONLINE (Mar. 27, 2023), https://lawreviewblog.uchicago.edu/2023/03/27/irion-kaminski-yakovleva/ [hereinafter Irion et al.] (the authors describe U.S. action as "rising "data protectionism" by the United States under a national security label").

[73] Kenneth Rogoff, *A US Ban on TikTok Could Damage the Idea of the Global Internet*, GUARDIAN (Mar. 29, 2023, 18.59 BST), https://www.theguardian.com/business/2023/mar/29/us-ban-tiktok-global-internet-china-tech-world (TikTok also captures American adult attention for an average of one hour per day).

[74] *See, e.g.*, Norman Pearlstine et al., *The War Against Huawei: Why the U.S. Is Trying to*

concern for individuals' data.

Grindr is an American dating web site for "gay, bi, trans and queer people," sixty percent of the shares of which were acquired by the Chinese company Beijing Kunlun Wanwei Technology Co., Ltd. (Kunlun).[75] This was seen as a national security concern, potentially related to a possible transfer back to China of sensitive personal data of U.S. intelligence and military personnel who happened to be Grindr users, where the Chinese government could access them through Grindr.[76] Indeed, Grindr's privacy policy was reported to have allowed sharing of personal data, which could include data about sexual identity, HIV status, and location with its parent company,[77] although its Chinese owner said that, because it was not owned by the Chinese government, the latter could not access its data.[78]

As a result of the controversy, Kunlun entered into a "National Security Agreement" with the Committee on Foreign Investment in the United States (CFIUS), by which it undertook commitments prohibiting personnel from accessing "relevant Grindr sensitive data," requiring it to keep Grindr headquarters and operations in the United States, with certain "CFIUS-approved personnel" on its board, and requiring it to sell its share of Grindr (which by then had risen to one hundred percent) by June 30, 2020.[79] Grindr was sold to San Vicente Acquisition in March 2020.[80]

2. TikTok

Similarly, with the TikTok case, the United States felt "unease" regarding how personal data collected by the popular Chinese app might be

---

Destroy China's Most Successful Brand, L.A. TIMES (Dec. 19, 2019), https://www.latimes.com/projects/la-fg-huawei-timeline/ (discussing a litany of U.S. actions against Huawei including a ban on supplying the company components and software without permission from the U.S. government).

[75] James Griffiths, *Gay Dating App Grindr Is the Latest Victim of US-China Tensions*, CNN (May 15, 2019, 8:47 PM EDT), https://edition.cnn.com/2019/05/14/tech/grindr-china-us-security/index.html.

[76] *See id.*

[77] Jacob Rosenberg, *The Trump Administration Apparently Considers Grindr a National Security Threat. What Is Going On?*, MOTHER JONES (Apr. 4, 2019), https://www.motherjones.com/politics/2019/04/the-trump-administration-apparently-considers-grindr-a-national-security-threat-what-is-going-on/.

[78] Guido Noto La Diega, *Should Grindr Users Worry About What China Will Do with Their Data?*, CONVERSATION (Aug. 31, 2018, 12:22 CEST), https://theconversation.com/should-grindr-users-worry-about-what-china-will-do-with-their-data-95972.

[79] International Trade Practice at Squire Patton Boggs (US) LLP, *CFIUS Filing in Mitigation: Beijing Kunlun Wanwei Technology Co. and Grindr Inc.*, XIII NAT'L L. REV. (June 19, 2019), https://www.natlawreview.com/article/cfius-filing-mitigation-beijing-kunlun-wanwei-technology-co-and-grindr-inc.

[80] Kori Hale, *Grindr's Chinese Owner Sells Gay Dating App Over U.S. Privacy Concerns For $600 Million*, FORBES (Mar. 26, 2020, 09:05am EDT), https://www.forbes.com/sites/korihale/2020/03/26/grindrs-chinese-owner-sells-gay-dating-app-over-us-privacy-concerns-for-600-million/.

used in China, thus finding itself in a similar situation to Europe at the time of the Snowden revelations, although now the danger was Chinese—and not U.S.—surveillance.[81] This national security turn regarding certain data transfers, already noted by at least one other commentator,[82] is reminiscent of the Chinese data protection law focus on national security discussed in Part III. Even though a TikTok U.S. General Manager asserted that the company stored U.S. user data on local United States servers with backup in Singapore and no storage in China, reports were made that the company was sending job applicant data from the United States to China.[83] Yet, the United States also found itself without data privacy protections, which might have helped deal with its concerns regarding national security related to Chinese government access to data, thus perhaps offering a new framing on how it should regulate in the area.[84] Furthermore, it might have effectively been encouraging "soft" data localization,[85] as evidenced by TikTok's assertion that it stored data on U.S. servers, even while the United States fought data localization elsewhere in the world.[86]

If data collection worried the United States generally, it could regulate this through omnibus data privacy legislation.[87] However, it has chosen an entirely different strategy, which aims to effectively limit certain personal data flows to China, despite the lack of a data privacy law with a data transfer restriction. In 2020, on grounds of national security, U.S. President Trump issued two executive orders banning transactions between persons subject to

---

[81] Marc Rotenberg, *Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection*, 26 EUR. L.J. 141, 150–152 (2020). *See also* Hoffman, *supra* note 49, at 609 (highlighting the similar legal ability of the U.S. and Chinese government to obtain personal data from companies and the importance of this given the "success and global reach of U.S. and Chinese technology companies").

[82] Yakovleva, *supra* note 71, at 204–05 (recalling that Americans' data are more and more being collected by Chinese-owned companies, feeding into a U.S. "national security narrative," which helps explain why in US law "national security is increasingly used as a rationale to control data and data flows to foreign countries," particularly, China).

[83] Hoffman, *supra* note 49, at 575–76.

[84] David Kaye & Gregory C. Shaffer, *Transnational Legal Ordering of Data, Disinformation, Privacy, and Speech*, 6 U.C. IRVINE J. INT'L TRANSNAT'L, & COMPAR. L. 1, 2 (2021).

[85] "Soft" data localization may be defined as "a legal regime that puts pressure on companies to localize, not by directly requiring localization of data or processes, but by making alternatives legally risky and thus potentially unwise." Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 772 (2020).

[86] While the "US government has sought to prevent the diffusion of data localization policies … Continued scrutiny about foreign access to US user data, exacerbated by technology bans, may motivate companies to store user data in the US." Apratim Vidyarthi & Rachel Hulvey, *Building Digital Walls and Making Speech and Internet Freedom (or Chinese Technology) Pay for It: An Assessment of the US Government's Attempts to Ban TikTok, WeChat, and Other Chinese Technology*, 17 INDIAN J.L. & TECH. 1, 39 (2021) [hereinafter Vidyarthgi & Hulvey].

[87] Gregory Shaffer, *Governing the Interface of US-China Trade Relations*, 115 AM. J. INT'L L. 622, 654 (2021).

U.S. jurisdiction and the popular Chinese application (app) TikTok, on the one hand, and Chinese messaging platform WeChat, on the other hand.[88] These were Executive Order No. 13,942 (TikTok Order),[89] and Executive Order No. 13,943 (WeChat Order),[90] which were both issued under the authority granted by the International Emergency Economic Powers Act (IEEPA).[91] The next year, TikTok's parent company, ByteDance, entered into a class action settlement agreement for $92 million, settling privacy claims by U.S. users under a variety of U.S. state and federal laws, including Illinois' Biometric Information Privacy Act. Such claims alleged that the Chinese app extracted a wide range of personal data for tracking and ad targeting.[92] There was a fear that these companies would transfer personal data of U.S. citizens to China, where it could be subject to data requests by the Chinese government, enabling it to "track federal employee's physical movements, build dossiers of personal information to blackmail U.S. citizens," and "conduct corporate espionage."[93]

In addition to the executive orders, Trump used CFIUS to attempt to force both TikTok and WeChat to cease business in the United States and to have TikTok change ownership. His actions led to litigation[94] and preliminary injunctions such as that in an action by TikTok—*TikTok Inc. v. Trump*—in which the Court enjoined Department of Commerce prohibitions

---

[88] Maanvi Singh, *Trump Bans US Transactions with Chinese-Owned TikTok and WeChat*, GUARDIAN (Aug. 7, 2020), https://www.theguardian.com/technology/2020/aug/06/us-senate-tiktok-ban.

[89] Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020) (Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain). (The order stated, "Specifically, the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States. At this time, action must be taken to address the threat posed by one mobile application in particular, TikTok.").

[90] Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 6, 2020) (Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain).

[91] 50 U.S.C. §§ 1701–1707. For a discussion of this use of the International Emergency Economic Powers Act, *see* Robert L. Rembert, *TikTok, WeChat, and National Security: Toward a U.S. Data Privacy Framework*, 74 OKLA. L. REV. 463, 465-67 (2022) [hereinafter Rembert].

[92] Bobby Allyn, *TikTok to Pay $92 million to Settle Class-Action Suit Over 'Theft' Of Personal Data*, NPR (Feb. 25, 2021), https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data; Morgan Sung, *That TikTok Notification About a Settlement Payment Isn't a Scam. Here's What to Know*, NBC News (Nov. 17, 2021), https://www.nbcnews.com/news/us-news/need-know-tiktoks-class-action-lawsuit-rcna5781.

[93] Rembert, *supra* note 91, at 465.

[94] Kristen Eichensehr (ed.), *United States Pursues Regulatory Actions Against TikTok and WeChat Over Data Security Concerns*, 115 AM. J. INT'L L. 124 (2021)

of certain transactions involving TikTok, under TikTok Order.[95] Eventually in June 2021, his successor, President Biden, revoked these two executive orders.[96]

Most recently, though, the chief administrative officer (CAO) of the U.S. House of Representatives, who had previously issued a "cyber advisory" due to TikTok's "lack of transparency in how it protects customer data," related to TikTok's harvesting identifiable data and storing them overseas.[97] The CAO established a ban on downloading the TikTok app on any House mobile device, and an order to delete the app when it is already on devices issued by the House.[98] This is one of several initiatives to limit TikTok use by state and government workers.[99] Furthermore, H.R. 2617, the "Consolidated Appropriations Act, 2023," which contains in its Division R the "No TikTok on Government Devices Act," was enacted after having been signed by President Biden on December 29, 2022.[100] It bans the use of TikTok on U.S. federal government devices.[101] However, this might not have been necessary, had the United States adopted comprehensive data privacy legislation with a restriction on certain personal data transfers, similar to that of the European Union. Finally, such moves creating "digital walls," may negatively impact the United States' ability to achieve its goal of obtaining the free flow of data around the world,[102] if that is still what it seeks.

C. Potential Federal Data Privacy Legislation to the Rescue?

Already, some legislators view federal data privacy legislation as part of the solution. The Subcommittee on Innovation, Data, and Commerce of the U.S. House of Representatives' Energy & Commerce Committee held a hearing on February 1, 2023, entitled "Economic Danger Zone: How America Competes to Win the Future Versus China."[103] In a memo for the

---

[95] TikTok Inc. v. Trump, 490 F.Supp. 3d 73, 86 (D.D.C. 2020). For a discussion of the procedure leading up to the preliminary injunction, *see, e.g.*, Christopher R. Taylor, *TikTok, Inc. v. Trump: Can TikTok's U.S. Operations Last?,* WAKE FOREST L. REV. CURRENT ISSUES BLOG (Oct. 15, 2020), http://www.wakeforestlawreview.com/2020/10/tiktok-inc-v-trump-can-tiktoks-u-s-operations-last/.

[96] Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021) ("Protecting Americans' Sensitive Data From Foreign Adversaries").

[97] Dan Milmo, *TikTok Banned on Devices Issued by US House of Representatives*, GUARDIAN (Dec. 28, 2022), https://www.theguardian.com/technology/2022/dec/28/tiktok-banned-on-devices-issued-by-us-house-of-representatives.

[98] *Id*.

[99] *Id*.

[100] *H.R. 2617 (117th): Consolidated Appropriations Act, 2023*, GOVTRACK, https://www.govtrack.us/congress/bills/117/hr2617 (last visited Jan. 4, 2023).

[101] Johana Bhuiyan, *Why Did the US Just Ban TikTok from Government-Issued Cellphones?*, GUARDIAN (Dec. 31, 2022), https://www.theguardian.com/technology/2022/dec/30/explainer-us-congress-tiktok-ban.

[102] Vidyarthgi & Hulvey, *supra* note 86, at 4.

[103] Energy & Commerce Chair Rodgers, Innovation, Data, and Commerce Subcommittee

hearing, and in reaction to "China's approach to data," Committee majority staff argued that, "[t]o remain competitive, the U.S. must ensure there are guardrails around any data sharing with Chinese companies."[104] Then, they proceeded to discuss the benefits of federal privacy legislation such as the proposed American Data Privacy and Protection Act (ADPPA), saying that it "would establish strong data security requirements for companies and limit the type of information that certain companies can collect transfer, and process."[105] Finally, the proposed ADPPA includes a requirement to notify individuals when their data or information is "sent to, transferred, or otherwise made available to China, as well as to other foreign threats including Russia, North Korea, and Iran."

Without going into the merits of the proposed legislation, which at this stage seems to have died, or at least stalled, in Congress,[106] it is clear that the ADPPA would have taken a small step back from absolute free flows of information by introducing some constraints-such as notifications-on certain cross-border data flows to China. It would also have taken away some of what might be perceived as the subjectiveness of the current case-by-case protection and establish objective standards for conditions to transfer. However, this does not preclude problematic situations with certain Chinese companies. As an example, although Europe has instituted data protection regulations, the European Commission has still asked its employees to uninstall TikTok from their employer-supplied devices due to data security concerns.[107]

Hearing: "Economic Danger Zone: How America Competes to Win the Future Versus China" (Feb. 1, 2023), https://energycommerce.house.gov/events/innovation-data-and-commerce-hearing-is-entitled-economic-danger-zone-how-america-competes-to-win-the-future-versus-china.

[104] *Economic Danger Zone: How America Competes to Win the Future Versus China: Hearing Before H. Comm. on Energy & Commerce, Subcomm. On Innovation, Data, and Commerce*, 118th Cong. (2023) (Committee Majority Staff Hearing Memo to Subcommittee Members), https://d1dth6e84htgma.cloudfront.net/Briefing_Memo_IDC_2023_02_01_1_a94f2f0063.pdf?updated_at=2023-01-30T15:42:00.604Z.

[105] *Id*.

[106] Müge Fazlioglu, U.S. Privacy Legislation in 2023: Something Old, Something New?, iapp (July 26, 2023), https://iapp.org/news/a/u-s-federal-privacy-legislation-in-2023-something-old-something-new/ ("While there is little sign that the American Data Privacy and Protection Act will be (re)introduced to Congress any time soon …"); *see also* Cobun Zweifel-Keegan, *A View from DC: Sectoral Privacy Updates Spread with Strengthened Student Standards*, IAPP (May 26, 2023), https://iapp.org/news/a/a-view-from-dc-sectoral-privacy-updates-spread-with-strengthened-student-standards/. One political explanation for the ADPPA's lack of advancement: "for the act to have passed, Congress would have had to agree to preempt state data privacy laws, which Nancy Pelosi, listening to constituents in California, refused to do." Margot Kaminski, *Toward Stronger Data Protection Laws*, DEMOCRACY J. (Spring, No. 68), https://democracyjournal.org/magazine/68/toward-stronger-data-protection-laws/ (last visited May 27, 2023).

[107] Mark Sweney, *European Commission Bans Staff Using TikTok on Work Devices over Security Fears*, GUARDIAN (Feb. 23, 2023), https://www.theguardian.com/technology/

An important trigger here for the United States is an economic shift: the dawning era of Chinese big tech. Previously, the United States could count on its citizens' data being stored domestically, or at least controlled by U.S.-based entities, given the predominance of Silicon Valley.[108] However, today with the growth in popularity of Chinese apps and Chinese e-commerce sellers, that is no longer the case. Today, consumer data may be obtained by Chinese companies operating in the open US market and be used to hone Chinese algorithms allowing them greater competitiveness.[109] These data in turn may be shared with the Chinese government[110] for use in its interest. Nonetheless, part of the question is how far the United States will go in seeking to approximate the EU-style prescriptive approach with conditional data transfers (covered in Part II), and how much national security concerns will impact its handling of data transfers, perhaps in a way closer to that of China (discussed in Part IV), for strategic concerns, but with the distinct U.S. legal culture of checks and balances. Is a paradigm shift underway?

D. Certain Practices of Chinese Firms Dealing in the United States

In Section B.2, this study touched upon TikTok's action against Trump to seek invalidation of Trump's executive order seeking prohibition of certain transactions with TikTok. One commentator posits, without citing the TikTok example, that more broadly there is an effort by Chinese companies to fight national security decisions by governments that threaten their business. This effort includes litigation but also employs lobbying, the media, diplomacy, and trade association action to achieve its ends.[111] The judge-

2023/feb/23/european-commission-bans-staff-from-using-tiktok-on-work-devices [hereinafter Sweney].

[108] Irion et al., *supra* note 72 (discussing the "data sovereignty by default" basis for the U.S. preference for free data flows, and citing Anupam Chander & Haochen Sun, *Sovereignty 2.0* (2021) (Georgetown L. Faculty Pubs. & Other Works. 2404; U. Hong Kong Faculty of L. Research Paper No. 2021/041). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904949).

[109] Aynne Kokas, *Platform Patrol: China, the United States, and the Global Battle for Data Security*, 77 J. ASIAN STUD. 923, 929 (2018) ("Platforms are gathering huge amounts of consumer data (and other forms of data) to build smarter algorithms …With open access to the US market and virtually no foreign competitors, Chinese firms are getting access to vast quantities of this data, largely because there is such limited protection of consumer data in the United States and many other countries around the world. … failure to get ahead of developments in the market may lead to a dramatic loss of American competitiveness in a key industrial sector.").

[110] AYNNE KOKAS, TRAFFICKING DATA: HOW CHINA IS WINNING THE BATTLE FOR DIGITAL SOVEREIGNTY 49 (2023) ("US firms with operations in China and Chinese firms operating in the United States are expanding the Chinese government's data oversight not just in the United States, but globally. Firms dependent on the Chinese market will continue to extract commercial data and share it with the Chinese government if US corporate and government leaders continue to allow the tech industry's financial interest to direct policy.").

[111] Ming Du, *How Chinese Companies Are Challenging National Security Decisions That Could Delay 5G Network Rollout*, CONVERSATION (Jan. 19, 2023), https://theconversation.

ordered end to a Montana ban on TikTok, where TikTok's parent ByteDance argued that it violated the First Amendment serves as an additional example.[112]

TikTok has been negotiating what it has called "Project Texas" with the CFIUS, as a form of "mitigation agreement," where compliance with it would be monitored by CFIUS.[113] The proposed agreement is reported to involve a TikTok U.S. subsidiary, created in July 2022, whose board would report to CFIUS, and would house employees accessing user data, which would be routed through Oracle Cloud in the United States.[114] TikTok says that all U.S. user data is already stored in that cloud, but that some U.S. user data will need to leave the United States to enable U.S. TikTok users to interact with TikTok users abroad, the potential cases of which have been vetted with CFIUS and will be monitored by Oracle, if the agreement is reached.[115] Obviously, at the heart of this proposed deal is data localization in the United States. Commenting on how the proposed deal would give the U.S. government a great deal of say on TikTok content moderation, journalist Mike Masnick mentions establishing privacy laws as a reasonable alternative.[116]

To take an example from another Chinese Big Tech company, for U.S. users, a section of the AliExpress privacy policy indicates that AliExpress E-Commerce One Pte. Ltd., incorporated in Singapore, is their data controller, and will store their data in the United States. It then proceeds to give information on specific rights under California and Nevada law.[117] Thus,

---

com/how-chinese-companies-are-challenging-national-security-decisions-that-could-delay-5g-network-rollout-195874. For a more detailed development of the issues, *see generally*, Ming Du, *Huawei Strikes Back: Challenging National Security Decisions Before Investment Arbitral Tribunals*, 37 EMORY INT'L L. REV. 1 (2022).

[112] Clyde Hughes, *Judge Halts Montana Law Banning TikTok on First Amendment Grounds*, UPI (Dec. 1, 2023, 8:59 AM), https://www.upi.com/Top_News/US/2023/12/01/tiktok-ban-montana-blocked/5881701437193/.

[113] Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*, LAWFARE (Jan. 26, 2023), https://www.lawfareblog.com/project-texas-details-tiktoks-plan-remain-operational-united-states#.

[114] *Id*. (the subsidiary is TikTok U.S. Data Security Inc., or USDS).

[115] *Id*. (the data fields of these cases of data vetted are described as "public data, interoperability data, and safety tools").

[116] Mike Masnick, *What State Action Doctrine? Biden Administration Renews Push For Deal With TikTok, Where US Government Would Oversee Content Moderation On TikTok*, TECHDIRT (Sept. 21, 2023), https://www.techdirt.com/2023/09/21/what-state-action-doctrine-biden-administration-renews-push-for-deal-with-tiktok-where-us-government-would-oversee-content-moderation-on-tiktok/ ("Honestly, what this reads as is the moral panic over China and TikTok so eating the brains of US officials that rather than saying 'hey, we should have privacy laws that block this,' they thought instead 'hey, that would be cool if we could just do all the things we accuse China of doing, but where we pull the strings.'").

[117] AliExpress.com Privacy Policy, ALIEXPRESS, ¶ K (Visitors from the United States), https://terms.alicdn.com/legal-agreement/terms/suit_bu1_aliexpress/suit_bu1_aliexpress201909171350_82407.html (last visited Jan. 21, 2023) [hereinafter AliExpress.com Privacy Policy].

effectively there is a certain degree of data localization in the United States, although it may strictly speaking be "soft" data localization,[118] albeit under a certain degree of constraint by regulators, depending on the case.

E. Conclusion to Part II

This study has shown in its Part I that, although the United States has no data transfer restrictions generally, or even specifically with regard to China, certain actions by the United States based on national security and on user privacy grounds, have served to limit certain data flows to China and have sometimes led to effective data localization in the United States by specific Chinese companies. In addition, U.S. action has resulted in pushback in the courts by TikTok. Yet, the United States' targeted case-by-case action involving a few Chinese companies does not yet amount to the largely applicable data transfer restrictions that exist in the European Union and China, for example, as may be illustrated by the *Schrems II* case discussed in Part III, the Chinese data localization requirements detailed in Part IV, and Chinese data transfer restrictions analyzed in Part V. However, proposed data privacy legislation in the United States could provide certain requirements for some transfers of personal data to China, such as notification, reminding us in a small way of data transfer restrictions in the other power blocs, to which this study turns now.

III. THE GDPR TRANSFER RESTRICTION APPLICABLE IN THE CONTEXT OF DATA EXPORTS TO CHINA

The European Union's GDPR, as successor legislation to the 1995 European Union Data Protection Directive (1995 Directive),[119] inherited a cross-border data transfer restriction from that prior instrument,[120] and recast it in its Articles 44 through 50.[121] That restriction was needed in order to avoid companies transferring data out of the European Union to circumnavigate the constraints of EU data protection law.[122] This is significant for China as it was the European Union's largest trade partner for

[118] For a definition of "soft" data localization, *see supra* note 85.

[119] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) [hereinafter 1995 Directive]. The GDPR repealed the 1995 Directive with effect from May 25, 2018. GDPR, *supra* note 54, art. 94(1).

[120] 1995 Directive, *supra* note 119, arts. 25 (Transfer of Personal Data to Third Countries) and 26 (Derogations).

[121] GDPR, *supra* note 54, arts. 44–50 (constituting its Chapter V (Transfers of Personal Data to Third Countries or International Organisations)).

[122] *See, e.g.*, OF PRIVACY AND POWER, *supra* note 2, at 129 ("This was intended to block an obvious loophole in EU law; without such a rule it would be easy for multinational corporations to transfer personal information on EU citizens to a third jurisdiction with weak privacy rules and process it there, doing an end run around EU privacy protections.").

its import of goods in 2021.[123] It is also important due to the role data play in international trade today.

Part III is divided into seven sections, the first of which details the GDPR's transfer restriction. The second section discusses the criteria for a country to obtain a Commission adequacy determination to allow for data flows (China does not benefit from such a determination today). The third section discusses various safeguards that may be used to allow transfers (as are required for data exports to China), the fourth section sets out various investigations that a data exporter and data importer must make when using safeguards, following the decision of the CJEU in the *Schrems II* case.[124] In the fifth section, supplementary measures that may be taken in potentially problematical legal settings, such as surveillance, in order to allow for transfers are briefly discussed, and the sixth section discusses certain practices of Chinese firms dealing in the European Union. The seventh section concludes this Part II.

A. The GDPR Data Transfer Restriction

Article 44 of the GDPR sets out the general principle for transfers and provides in part that any transfer of EU personal data to a third country for processing must respect the conditions in Chapter V of the GDPR on transfers, "including for onward transfers of personal data from the third country . . . to another third country . . . ."[125] First, note that the concept of processing in the GDPR is a broad one, encompassing almost any operation that may be carried out on personal data.[126] Next, a third country is a country outside of the European Union,[127] such as the United States or China, which is logical because one of the two overarching goals of the GDPR is to allow the free movement of such data within the European Union,[128] so long as requirements for processing are met,[129] including respect of the GDPR's data

---

[123] *China-EU - International Trade in Goods Statistics*, EUROSTAT (Nov. 6, 2023), https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics.

[124] Schrems II, *supra* note 47.

[125] GDPR, *supra* note 54, art. 44 (General Principle for Transfers).

[126] The definition of "processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." *Id.* art. 4(2).

[127] *See id.* at recital 101. Here, the "European Union" should now be read to extend to the entire European Economic Area (EEA), encompassing the EU Member States, as well as Iceland, Liechtenstein, and Norway, as such countries have adopted the GDPR. *See Transatlantic Data Transfer Compliance*, *supra* note 24, at 167–68.

[128] GDPR, *supra* note 54, at art. 1(3) ("The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.").

[129] This includes the requirement of a lawful basis for the processing. *See id.* art. 6.

protection principles.[130] An important condition is that an adequacy decision for the importing third country or international organization exist (Section B), or that an appropriate safeguard or a derogation (Section C) is available to the controller or processor exporting the data.

B. The Commission Adequacy Decision and Its Relevant Criteria

If the Commission determines that a third country or an international organization sufficiently protects personal data, then it may issue an adequacy decision in favor of such entity. When the jurisdiction or international organization importing EU personal data benefits from an adequacy decision, the GDPR data transfer restriction does not apply.[131] However, the problem is that very few jurisdictions benefit today from a Commission adequacy decision. These are: Andorra, Argentina, Canada (for commercial organizations, which are subject to the PIPEDA legislation), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea (South Korea), Switzerland, the United Kingdom, and Uruguay.[132] While China does not figure on this list, U.S. "commercial organisations participating in the EU-US Data Privacy Framework" do, as the Commission recently issued its adequacy decision for transfers to the United States under the EU-U.S. Data Privacy Framework,[133] which thus replaces the EU-U.S. Privacy Shield framework, invalidated by the CJEU in 2020 in its *Schrems II* decision.[134]

The criteria for an adequacy decision of the Commission are set out in the GDPR, and these will be applied to the Chinese context by this study in its Part V. These are:

> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the

[130] Those principles are largely contained in Article 5 of the GDPR (lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability). *Id.* art. 5. Broadly speaking, they are evolutions of the U.S. HEW's fair information practice principles (FIPPs), which were inspired by both European and American law, and became influential internationally. *Obstacles to Transatlantic Harmonization*, *supra* note 51, at 412–414.

[131] "Such a transfer shall not require any specific authorisation." GDPR, *supra* note 54, art. 45(1).

[132] *Adequacy Decisions*, EUR COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Feb. 10, 2024).

[133] Commission Implementing Decision EU 2023/1795 of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework, 2023 O.J. (L 231) 118 (Sept 20, 2023) [hereinafter EU-US Data Privacy Framework Decision].

[134] Schrems II, *supra* note 47, at para. 201.

> implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.[135]

Thus, the analysis is based on (i) the legal system of the destination country (rule of law, legislation, case-law and data subject rights and remedies), (ii) the fact that it has one or more independent data protection authorities or not, and (iii) its international commitments in data protection. As part of point (i), public authorities' access to personal data is considered. In the Adequacy Referential of the advisory group Article 29 Data Protection Working Party (WP29),[136] which was endorsed by its successor, the European Data Protection Board (EDPB),[137] WP29 highlighted the two-level analysis at play: first, the content of applicable rules must provide an "adequate level of protection," and the rules must be effective in practice, that is, they must be enforceable and followed.[138]

To have an adequate level of protection, the third country's protection must be "essentially equivalent" to that of the European Union—that is, the core (or essential) requirements of the GDPR must be present, although it does not need to constitute a mirror image of the GDPR.[139] Basic content that

---

[135] GDPR, *supra* note 54, art. 45(2).

[136] ARTICLE 29 DATA PROT. WORKING PARTY, *Adequacy Referential*, WP 254 REV.01 (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/items/614108 [hereinafter *Adequacy Referential*].

[137] *Our Work & Tools: Guidelines, Recommendations, Best Practices: Endorsed WP29 Guidelines*, EUR. DATA PROT. BD., https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en (last visited Jan. 9, 2023) (the Adequacy Referential appears as item 15).

[138] *Adequacy Referential*, *supra* note 136, ch. 1.

[139] *Id.*

must be included in the third country's system include certain basic data protection principles such as legitimate bases for data processing, set out clearly, purpose limitation, data quality requirements, limitation on data retention, data security, transparency, certain data subject rights (e.g., to access, rectification, erasure and to object), and restrictions on further data transfers based on an adequacy requirement.[140] Also, where sensitive data exists, specific safeguards should apply, such as explicit consent for processing. Furthermore, a good level of compliance should be ensured by the system, and data controllers should be required to comply and be able to prove it.[141]

The Commission has set out criteria for deciding with which nations to prioritize discussions about establishing adequacy decisions:

> (i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
>
> (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
>
> (iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
>
> (iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.[142]

Obviously, geopolitics enters the analysis in most of these points. While the Commission mentioned targets for adequacy discussions of Japan and Korea—which now benefit from adequacy decisions since implemented—and India, Latin American countries (especially Mercosur members), and countries in the European neighborhood, China is not mentioned.[143] Specific issues related to the potential of an adequacy decision for China are discussed in Part III.

C. Appropriate Safeguards to Preserve Data Subject Rights

In cases of exportation of personal data from the European Union to third countries or international organizations where no Commission adequacy decision applies, such as is the case for China, then the controller

---

[140] *Id.* at ch. 3.

[141] *Id.*

[142] *Communication from the Commission to the European Parliament and the Council*, EUR COMM'N, at 8, (Oct. 1, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN (citation omitted).

[143] *Id.* at 10.

or the processor exporting the data must provide appropriate safeguards to transfer the data,[144] or, failing that, a derogation must apply.[145] Reliance on appropriate safeguards is subject to the condition that "enforceable data subject rights and effective legal remedies for data subjects are available."[146] The EU Charter of Fundamental Rights provides in relevant part that:

> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.[147]

Indeed, having effective judicial review in place is "inherent in the existence of the rule of law."[148] The rule of law is the first of the criteria for an adequacy decision listed in the GDPR.[149]

The appropriate safeguards that are available, without authorization from a supervisory authority, include, among others, binding corporate rules and standard data protection clauses.[150] In addition, with supervisory authority authorization, appropriate safeguards may be provided by contractual clauses or "provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights."[151] Furthermore, in certain specific situations, derogations may be relied upon for cross-border transfers, as detailed in Article 49 of the GDPR.[152] Those derogations are to be used with parsimony and are interpreted restrictively.[153] However, the most popular "appropriate safeguard," or transfer tool by far is that listed in Article 46(2)(c) of the GDPR—standard data protection clauses adopted by the Commission (or EU SCCs).[154] Other transfer mechanisms are only used by a

---

[144] GDPR, *supra* note 54, art. 46(1).

[145] *Id*. art. 49(1).

[146] *Id*. art. 46(1).

[147] Charter of Fundamental Rights of the European Union art. 47, 2000 O.J. (C 364) 1.

[148] Case C-362/14, Maximilian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 95 (Oct. 6, 2015). [hereinafter Schrems I].

[149] GDPR, *supra* note 54, art. 45(2)(a).

[150] *Id*. art. 46(2).

[151] *Id*. art. 46(3).

[152] *Id*. art. 49(1).

[153] Christopher Kuner, *Article 49. Derogations for Specific Situations*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 841, 846 (Christophe Kuner, Lee A. Bygrave, & Christopher Docksey, eds., 2020).

[154] One trade association survey showed that eighty-five percent of companies surveyed estimated that they used SCCs as a transfer mechanism. Schrems II Impact Survey Report 5 (Digital Europe, 2020), https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.

relatively small minority of companies, according to a trade association survey.[155] Moreover, the 2020 *Schrems II* case law requires an additional step—a transfer assessment—before controllers may export EU data to countries that do not benefit from an adequacy decision, such as China, as is discussed in Part II.D.

D. Schrems II and Transfer Assessments for Exportation of Data to China

Like the proceedings leading to the *Schrems I* decision[156] before it, the *Schrems II* action was brought by plaintiff Maximilian Schrems to stop personal data exports by Facebook to the United States, where they would potentially be subject to access by U.S. authorities.[157] However, the transfer mechanisms employed in the two cases were different. In *Schrems I*, the CJEU invalidated[158] the Commission's adequacy decision[159] involving the Safe Harbor framework between the United States and the European Union, based on the lack of procedural protections for EU data subjects when their data was exported to the United States under the framework.[160] In many ways the *Schrems II* case was based on similar reasoning but aimed at invalidating the appropriate safeguards of standard data protection clauses (EU SCCs), instead.[161] However, the CJEU took the opportunity to invalidate the Commission adequacy decision of the Safe Harbor's successor—the EU-U.S. Privacy Shield framework negotiated after the *Schrems I* decision[162]—and left the EU SCCs as valid potential appropriate safeguards for personal data transfers, under certain conditions,[163] which are also applicable to other appropriate safeguards, such as binding corporate rules (EU BCR).[164] Yet,

---

[155] The survey shows these used by five percent of companies. *Id*. at 8.

[156] Schrems I, *supra* note 148.

[157] *See, e.g*., Fahey, *supra* note 24, at 136.

[158] Schrems II, *supra* note 47, at para. 201.

[159] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 O.J. (L 215) 7 [hereinafter Safe Harbor Decision].

[160] Schrems II, *supra* note 47, at para. 192 ("[N]either PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy.").

[161] *See, e.g*., THE EU AS A GLOBAL DIGITAL Actor, *supra* note 24, at 136.

[162] Schrems II, *supra* note 47, at para. 201 ("In light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid.").

[163] *Id*. at para. 134 ("It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.").

[164] This would be the case for the alternative appropriate safeguard of EU BCRs, for example. *See, e.g*., Tracol, *supra* note 24, at 10 ("The personal data exporter and importer both bear . . . the onus to assess whether the legislation of the third country of destination enables the data importer to comply with the guarantees provided by the SCCs or the BCRs in practice

Meta Ireland's (Facebook) transfer of personal data from the European Union to the United States, even under the EU SCCs in conjunction with supplementary measures, was deemed inadequate in addressing the risks to data subjects' fundamental rights, as required by *Schrems II*. As a result, in May 2023, the Irish supervisory authority ordered a suspension of such data transfers within five months and a ceasing of the processing of the data within six months, in addition to the assessment of a €1.2 billion administrative fine.[165] In part, this could have been expected as Meta would be considered an "electronic communications service provider" subject to U.S. surveillance law requirements.[166] The Safe Harbor and the Privacy Shield frameworks only concerned transfers to the United States,[167] likely as the result of a compromise position reached owing to the importance of the transatlantic commercial relationship.[168] Such agreements are unlikely to be replicated in other contexts, as this enters the realm of geopolitics. Therefore, in this study, which deals with data flows to and from China, the conditions for the use of appropriate safeguards are of particular interest.

Under *Schrems II*, the CJEU mandated an investigation into the laws of the destination or importing country when EU SCCs, or other appropriate safeguards, are used for cross-border transfer of personal data, when no adequacy decision exists.[169] Following the CJEU's decision and its logic, a similar transfer assessment would need to be made with respect to China to allow the export of personal data there under an appropriate safeguard. To begin with, the assessment of the adequacy of the protection for transfer—

before transferring any personal data to this third state.").

[165] Data Protection Commission Press Release, Data Protection Commission Announces Conclusion of Inquiry into Meta Ireland (May 22, 2023), https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.

[166] W. Gregory Voss, Airline Commercial Use of EU Personal Data in the Context of the GDPR, *British Airways* and *Schrems II*, 19 COLO. TECH. L.J. 377, 420–21 (2021).

[167] The Safe Harbor adequacy decision affirms that the "'Safe Harbor Privacy Principles' . . . are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States." Safe Harbor Decision, *supra* note 159, art. 1(1).

The Privacy Shield adequacy decision provides that, "personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the 'Privacy Shield List' . . . ." Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, O.J. (L 207) 1, art. 1(3).

[168] Maria Helen Murphy, *Assessing the Implications of Schrems II for EU–US Data Flow*, 71 ICLQ 245, 246 (2022) ("The EU, as represented by the Commission, has sought compromise in its data transfer negotiations with the US—as evidenced by both the Safe Harbour and Privacy Shield agreements . . . . The impetus to reach compromise can be explained by the fact that transfers of personal data between the EU and the US are an integral element of the transatlantic commercial relationship.").

[169] Schrems II, *supra* note 47, at para. 134.

with a requirement of essentially equivalent protection to that provided in the European Union by the GDPR, read in the light of the Charter—must take into consideration the EU SCCs (or other appropriate safeguards, as the case may be).

In addition, in the case of any access to the personal data by public authorities in the destination country (in our case, China) aspects of that country's legal system (here, again, the Chinese legal system) must be assessed, including the factors for adequacy from GDPR Article 45(2), which are set out in Section B above.[170] If the relevant national data regulator or "supervisory authority" is of the opinion that the EU SCCs cannot be complied within the destination country in this matter, China, or that protection of the data at the required standards cannot be ensured, it must suspend or prohibit the transfer if the controller or processor has not done so itself.[171] As EU SCCs cannot bind public authorities, "it may prove necessary to supplement the guarantees contained in those" EU SCCs.[172] The determination of this necessity is first of all a matter for the data exporter to make.[173] The data exporter must suspend or terminate the transfer when they are unable to take such necessary additional measures to guarantee protection.[174] Also, where EU SCCs cannot be respected or are breached, the transfers of data pursuant to them must be suspended or prohibited.[175]

These case law requirements are reflected in the new EU SCC decision (2021 EU SCC Decision) that was approved by the Commission and is now required to be used for that form of the transfer mechanism.[176] In the 2021 EU SCC Decision, the parties warrant that "they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations" pursuant to the EU SCCs.[177] In order to make such a warranty, the parties, in the case of our study, need to verify Chinese law and practice to ensure that they "respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1)" of the GDPR and do

[170] *Id*. at para. 105.
[171] *Id*. at para. 121.
[172] *Id*. at para. 132.
[173] *Id*. at para. 134.
[174] *Id*. at para. 135.
[175] *Id*. at para. 137.
[176] *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, 2021 O.J. (L 199) at 31 (June 7, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN [hereinafter EU SCC Implementing Decision].
[177] *Id*. annex cl. 14(a).

not contradict the EU SCCs.[178]

If the data importer cannot comply with the SCCs, it must promptly inform the data exporter,[179] and the latter must suspend the transfer until the importer can again comply or the contract is terminated.[180] Furthermore, if the data importer is required to disclose the personal data transferred to public authorities, specifically Chinese authorities, or if these authorities can access the data directly, the data importer must notify the data exporter of such fact.[181]

E. Supplementary Measures

In Section D above, this study discussed the *Schrems II* requirement that in certain circumstances data exporters use supplemental measures to ensure that transfers of personal data pursuant to appropriate safeguards provide adequate data protection. The analysis on whether supplemental measures are necessary may be made using a "roadmap" provided by the EDPB,[182] which includes as a third step to: "Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer."[183] Here, the data exporter, with the cooperation of the importer, if necessary, assesses if the destination country's (in this case, China's) laws or practices limit the appropriate safeguard's effectiveness. To do this, the exporter should consider, "whether public authorities of the third country of your importer may seek to access the data with or without the data importer's knowledge, in light of legislation, practice and reported precedents" and if such public authorities "may be able to access the data through the data importer or through the telecommunications providers or communication channels in light of legislation, legal powers, technical, financial, and human resources at the disposal and of reported precedents."[184]

With respect to destination countries that practice surveillance measures, the EDPB established recommendations on European Essential Guarantees (EEG), "to provide elements to examine, whether surveillance measures allowing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be regarded as a justifiable interference or not."[185] These EEG are: "A.

---

[178] *Id*.

[179] *Id*. annex cl. 16(a).

[180] *Id*. annex cl. 16(b).

[181] *Id*. annex cl. 15.1(a).

[182] EUR. DATA PROT. BD., *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data: Version 2.0*, at 10–25 (June 18, 2021), https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en [hereinafter *Recommendations 01/2020 V.2*].

[183] *Id*. at 14–21.

[184] *Id*. at 14.

[185] EUR. DATA PROT. BD., *Recommendations 02/2020 on the European Essential*

Processing should be based on clear, precise and accessible rules, B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated, C. An independent oversight mechanism should exist," and "D. Effective remedies need to be available to the individual."[186] These elements must be assessed together "on an overall basis" and will lead to one of two conclusions: either, the third country's legislation does not meet EEG requirements, and so does not offer essentially equivalent data protection, or that it does satisfy the EEG.[187]

If the analysis leads to the former conclusion, "this would imply to ensure that the law at stake will not impinge on the guarantees and safeguards surrounding the transfer, in order for a level of protection essentially equivalent to that guaranteed within the EU to be still provided."[188] This may require implementation of "adequate supplementary measures," if possible, for data transfers to the destination to proceed.[189] In such a case, the data exporter, with the help of the data importer, will need to determine whether supplementary measures, taken together with the transfer tool, allow for an equivalent level of data protection as that guaranteed in the European Union.[190] Without going into detail, such supplementary measures may include additional contractual commitments, technical measures like encryption and pseudonymization, and organizational measures such as internal policies, organizational methods, and standards.[191] However, in certain cases supplementary measures will not be enough. Data controllers should keep in mind the Irish supervisory authorities' May 2023 decision against Meta (Facebook) in this regard.

F. EU Personal Data That Transit Through the United States Prior to Transfer to China

One additional twist in the law regarding data transfers that must be included in this study's analysis is the case of EU personal data that flow to the United States, prior to being transferred to China. The legal treatment of such flows depends on the circumstances of the transmitting through the United States. If, for example, a data controller in the United States collects data directly from an EU data subject under Article 3(2) of the GDPR, then the GDPR applies to the transfer from the United States to China. This means that Chapter V of the GDPR, which includes the GDPR's data transfer

---

Guarantees for surveillance measures, at 5 (Nov. 10, 2020), https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.

[186] *Id*. at 8.

[187] *Id*. at 15.

[188] *Id*.

[189] *Recommendations 01/2020 V.2*, *supra* note 182, at 17.

[190] *Id*. at 21.

[191] *Id*. at 28–46 (providing examples that enter into each of these categories with conditions for their effectiveness).

restriction, would apply to the transfer to China.[192] Concretely, a transfer mechanism would then need to be relied on for that transfer to China (such as EU SCCs).

However, if the EU personal data have been transferred from the European Union to the United States other than under Article 3(2), for example, using EU SCCs or in connection with the EU-US Data Privacy Framework Decision,[193] then the conditions of that basis of transfer for onward transfers contained in the EU-U.S. Data Privacy Framework Principles issued by the U.S. Department of Commerce and annexed to the EU-US Data Privacy Framework Decision[194] must be respected. These provide for accountability requirements that include notice and choice provisions allowing the data subject to opt-out from disclosure to a third party or for use for a materially different purpose, when the recipient is acting as a controller.[195] Where the recipient acts as an agent, the organization must ensure that such agent "is obligated to provide at least the same level of privacy protection" as required by the Data Privacy Framework Principles.[196]

In the case that EU SCCs are the basis for transfer to the United States, the provisions of the EU SCC for onward transfers must be respected.[197] This involves giving the data subject notice, and the onward transfer to a third party is only allowed "if the third party accedes to the standard contractual clauses, if the continuity of protection is ensured otherwise, or in specific situations, such as on the basis of the explicit, informed consent of the data subject."[198] Thus, the fact that data transit from the European Union through the United States takes nothing away from the need to respect EU law (in the case of export subject to Article 3(2) of the GDPR) or data protection principles (in the case of an export using transfer mechanisms).

G. Certain Practices of Chinese Firms Dealing in the European Union

According to one commentator, Alibaba, TikTok, and WeChat have modified their privacy policies for Europe.[199] For example, Alibaba Group's

---

[192] EUR. DATA PROT. BD., *Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR: Version 2.0*, at 7–8 (Feb. 14, 2023), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.

[193] EU-US Data Privacy Framework Decision, *supra* note 133.

[194] *Id*. annex I (EU-U.S. Data Privacy Framework Principles Issued by the U.S. Department of Commerce).

[195] *Id*. annex I, para II.3(a).

[196] *Id*. annex I, para. II.3(b)(ii). (These requirements, which are unchanged from those of the Privacy Shield were reproduced with respect to that earlier instrument in *Cross-Border Data Flows*, *supra* note 7, at 526–27).

[197] EU SCC Implementing Decision, *supra* note 177, annex module one cl. 8.7, module two cl. 8.8, and module three cl. 8.8. (For a brief discussion of certain obligations under these clauses, see *Transatlantic Data Transfer Compliance*, *supra* note 24, at 184–85).

[198] *Id*. at recital (11).

[199] Stanislav Gubenko, *Tracing the Expansive Effect of the GDPR in the Third Countries.*

AliExpress, which engages in business-to-consumer sales, provides a menu item entitled "Information for EU consumers" that takes you to a document on consumer rights under EU law.[200] Another menu item for the privacy policy contains a section for users from the European Economic Areas (EEA) and the United Kingdom, which informs users that their data controller is a Singapore-incorporated company, Alibaba.com Singapore E-Commerce Private Limited.[201] In addition, sellers on the platform are said to also be controllers for sales made with them, and information on data subject rights is provided.[202] Without specifying which jurisdiction is the applicable one for EU customers, AliExpress discloses that it stores data in "the United States, Russia, Germany, China and/or Singapore, depending on the country you are located in," that it makes data transfers "among the above-mentioned countries," and that it takes measures to ensure personal data protection, such as the use of standard contractual clauses or "other mechanism provided for in the applicable law."[203] It would be logical for U.S. data to be stored in the United States, for Russian data to be stored in Russia, EU data to be stored in Germany, and so on, but the privacy policy does not specify this, and so more information is needed. In addition, TikTok's parent company announced it was establishing three more data centers in Europe, to ensure that user data was not exported to foreign countries such as China.[204]

Furthermore, an example of Controller BCR that would allow transfers of data to member entities in China received a positive opinion from the EDPB. The BCR is that of the Internet Initiative Japan Group, and although the Group itself is not China-based, it has Chinese operations, and was approved by the lead supervisory authority of North Rhine-Westphalia (Germany). In its assessment, the EDPB noted that this EU BCR covers transfers from group members in Europe to group members in China, among other countries.[205] The use of this EU BCR is made conditional on verifications made in conformity with the requirements of the *Schrems II* decision and that it is found that that the guarantees for the protection of

The Cases of Russia, Ukraine and China, PEACE HUM. RTS. GOVERNANCE 6(1) at 79, 87 (2022), https://doi.org/10.14658/pupj-phrg-2022-1-4.

[200] *Statutory Rights for EU Consumers*, ALIEXPRESS https://sale.aliexpress.com/__pc/QnoLFBVfqY.htm?spm=a2g0o.home.0.0.650c2145loCHm0 (last visited Jan. 21, 2023).

[201] AliExpress.com Privacy Policy, *supra* note 117, at para. J.

[202] *Id*.

[203] *Id*. at para. M (International Transfers of Personal Data).

[204] Sweney, *supra* note 107.

[205] EUR. DATA PROT. BD., *Opinion 26/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Controller Binding Corporate Rules of the Internet Initiative Japan Group*, at 5 (2021), https://edpb.europa.eu/system/files/2021-08/edpb_opinion_202126_iij_bcr-c_en.pdf.

personal data contained in the BCRs may in practice be respected, failing which the use of supplementary measures should be assessed:

> … it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights.[206]

A similar Processor EU BCR was also approved by the EDPB on the same day.[207] These two EU BCRs were the only approved EU BCRs under the GDPR that mention China that were identified in this study, although due to the global nature of the economy, other groups benefitting from approved EU BCRs certainly have operations in China, too. The test, though, is whether personal data can be exported to China and meet the conditions of the relevant EU BCR under the *Schrems II* assessment. Part III sheds light on this point.

H. Conclusion to Part III

In Part III, this study demonstrated that an important element of the GDPR related to data transfers is the data transfer restriction. The data transfer restriction requires either an adequacy determination or appropriate safeguards in order to allow any such transfer and to protect data subject rights in the destination country. China does not benefit from a Commission adequacy decision. Thus, in order for a transfer to occur, a data exporter in the European Union must, in cooperation with the data importer, establish appropriate safeguards for an export of personal data to China. However, the legal situation in China must be investigated to ensure that any such safeguards can be respected by the Chinese importer. Depending on that analysis, the safeguards may need to be accompanied by supplementary measures, or, if the parties determine that the conditions necessary for compliance with the safeguards do not exist, halt the transfers. Such an analysis will involve an investigation of Chinese law and practice. In Part IV, this study will look at Chinese data law, in the context of hopes for an adequacy decision benefitting the country, and with respect to the need for any supplementary measures.

---

[206] *Id*. at 5–6.

[207] EUR. DATA PROT. BD., *Opinion 27/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Processor Binding Corporate Rules of the Internet Initiative Japan Group* at 5 (2021), https://edpb.europa.eu/system/files/2021-08/edpb_opinion_202127_iij_bcr-p_en.pdf.

IV. CHINESE DATA PROTECTION LAW: A TRANSFER IMPACT ASSESSMENT

Since *Schrems II*, data exporters must perform transfer impact assessments ("TIAs") to demonstrate that when EU personal data is transferred, it benefits from adequate data protection when using transfer mechanisms such as EU SCCs or EU BCRs to send data to countries that do not benefit from an adequacy determination.[208] TIAs are performed by the data controller or processor and must consider, among other issues, whether the laws of the receiving country would allow government agencies to access the personal data in a way that does not respect the essence of fundamental rights and freedoms of data subjects. For example, generalized surveillance would not allow the importer to respect obligations under the transfer mechanism.[209] The TIA is motivated by the requirements of the CJEU *Schrems II* decision, the EDPB's recommendations,[210] and is called for in the 2021 version of the EU SCCs.

The TIA process requires an analysis of the destination country's legislation, access to the data by public authorities, and documentation of the assessment.[211] It emerged as a term-of-art to describe the process of analyzing the impact on privacy of transmitting personal information from the European Economic Area (EEA) to a country without a Commission adequacy decision.[212] TIAs should be conducted on a case-by-case basis and consider the specific safeguards applicable to the data transfer.[213] For the purpose of this study, the analysis pertains to the legislation of the importer's country, which is China in this case.

The level of protection for personal information against private actors in China is approaching that of European standards in several ways. A few years ago, there was only a trend toward greater approximation of EU law in China. The trend was met with lots of skepticism, which is understandable given the polemics about mass surveillance in China. However, this trend has now been widely demonstrated and accepted throughout the country.[214] An important element of context to understand the Chinese approach to data protection is that it is developed in reaction to a growth of the digital

---

[208] *See supra*, Part III (referring to the investigation of the laws of the importing country necessary following the *Schrems II* decision).

[209] *See Transatlantic Data Transfer Compliance*, *supra* note 24, at 507.

[210] *Recommendations 01/2020 V.2*, *supra* note 182.

[211] David A. Zetoony, *What Exactly Is a "Transfer Impact Assessment" (TIA), and Where the Heck Did It Come from?*, THE NATIONAL LAW REVIEW (Mar. 30, 2022), https://www.natlawreview.com/article/what-exactly-transfer-impact-assessment-tia-and-where-heck-did-it-come.

[212] *Id*.

[213] For examples of templates to carry out a TIA, *see* Transfer Impact Assessment Templates, IAPP (Sept. 1, 2021), https://iapp.org/resources/article/transfer-impact-assessment-templates/.

[214] *See, e.g.*, THE EU AS A GLOBAL DIGITAL ACTOR, *supra* note 24, at 178–79.

economy at a break-neck pace, supported by national policies;[215] a development that has also allowed the State to increase its mass-surveillance and spurs skepticism among researchers about China's enforcement of its rules, to the extent that it is advantageous both politically and economically as data protection itself in China does not have the strength of an EU fundamental right.[216] Significant challenges remain, among them enforcement and government access to personal data. While the first is not specific to China and can be tackled with time, effort, and resources, the second is more likely to remain part of the Chinese approach to data protection. Nevertheless, at this stage, the intellectual exercise of a TIA, and the preliminary assessment of the likelihood for China to benefit from an EC adequacy decision, will help draw a better picture of exactly where we are.

Part IV is divided into three sections. The first section details the main elements of China's legal framework on data protection. The second section assesses the important adequacy criterion of the rule of law with respect to China and in the context of government access to data. The third section provides a conclusion for Part IV.

A. China's Legal Framework on Data Protection: Convergence Towards GDPR But With Chinese Characteristics

The evolution of personal data protection rules in China is recent but rapidly evolving, forced by the fast-paced informatization of society and the government's concerns related to it.[217] The initial approach in the 2000s was very light-touch and far from the more stringent European laws. It was even labeled as "piecemeal and incoherent" by researchers.[218] But gradually, China ramped up its data privacy efforts through the enactment of several laws and guidelines, each of those new rules bringing more guarantees to the protection of personal information of individuals.[219] This new direction is part of the larger objective to rein in the tech sector with a stronger legal framework in several areas, from antitrust to cybersecurity.[220]

---

[215] Bo Zhao & Yang Feng, *Mapping the Development of China's Data Protection Law: Major Actors, Core Values, and Shifting Power Relations*, 40 COMPUT. L. & SEC. REV. 1, 9 (2021).

[216] *Id*. at 11–12.

[217] Rogier Creemers, *China's Emerging Data Protection Framework*, 8 J. CYBERSECURITY 2 (2022), https://doi.org/10.1093/cybsec/tyac011 (last visited Jan. 22, 2023) [hereinafter Creemers]. Creemers identifies several intertwined strands, namely the emergence of digitized government systems; the development of a digital economy driven by large platform companies (built on personal data processing); the rise of the economic value of data (and consequent black markets); and the growth of cyberattacks and various data breaches.

[218] Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIV. L. 68, 72 (2012) [hereinafter *The Influence of European Data Privacy Standards Outside Europe*].

[219] *See generally* Pernot-Leplay, *supra* note 46.

[220] Eva Xiao, *China Set to Pass One of the World's Strictest Data-Privacy Laws*, WALL ST. J. (Aug. 17, 2021), https://www.wsj.com/articles/china-set-to-pass-one-of-the-worlds-

From enacting only sectoral rules with light protections at first, China later leaned more and more towards the EU model with each new law, a phenomenon described in comparative law literature as a "legal transplantation."[221] But, while legal transplantation studies and observes the movement of rules across jurisdictions, the actual outcomes of a transplant will vary depending on the local context. Domestic specificities are indeed salient in the case of China,[222] and the European Commission considers these outcomes when granting adequacy decisions.[223] Today, the legal framework for data privacy in China is more comprehensive than those of many countries, including the United States.[224] However, a strong dichotomy still exists between privacy from private actors and privacy from the government as a consequence of China's broader political and legal context, in a way more or less contrary to that of the United States.

This paradox between increased protection from private actors and the reluctance to strictly regulate the State's use of personal data is perhaps what best defines "data protection with Chinese characteristics," along with its strong ties to national security and the related restrictions on data transfers.[225] These issues are handled in recent Chinese data privacy regulation detailed in this Section A. First, the 2017 Cybersecurity Law is introduced, followed by the 2019 Multi-Level Protection Scheme and the 2021 Data Security Law. Then, the important Personal Information Protection Law is studied. Other laws that mainly provide requirements for cybersecurity or only indirectly impact personal information protection, such as the new Anti-Espionage Law from April 2023, are out of scope of this article.

1. Cybersecurity Law (2017)

The Cybersecurity Law (CSL) was enacted on November 7, 2016, by the Standing Committee of the National People's Congress and came into force on June 1, 2017.[226] It is a major milestone in China's cybersecurity and

strictest-data-privacy-laws-11629201927.

[221] *See generally* ALAN WATSON, LEGAL TRANSPLANTS: AN APPROACH TO COMPARATIVE LAW (1st ed. 1974). For an additional discussion on the legal transplantation process, generally, outside of the Chinese context, *see* James M. Cooper, *Competing Legal Cultures and Legal Reform: The Battle of Chile*, 29 MICH. J. INT'L L. 501, 511(2008) (describing the process as involving "the adoption of, adaptation to, incorporation of, or reference to legal cultures from abroad" (citations omitted).

[222] Creemers, *supra* note 217, at 2.

[223] *See infra*, Part IV.B.

[224] Ashley Gold, *New China Privacy Law Leaves U.S. Behind — and Tech Companies Confused*, AXIOS (Nov. 23, 2021), https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind. *See also* Alexandra S. Levine, *'Deeply alarmed': China Now Ahead of U.S. on Privacy Law*, POLITICO (July 8, 2021 08:30 AM EDT), https://www.politico.com/newsletters/politico-china-watcher/2021/07/08/deeply-alarmed-china-now-ahead-of-us-on-privacy-law-493497.

[225] *See infra* Part V.

[226] Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ (中华人民共和国网络安全法)

data protection system, with a large array of requirements for network operators. It mandates the protection of "important data," especially where critical information infrastructure operators and national security may be concerned, but also data privacy and the protection of individuals. The CSL is the basis for the later regulations that are the Multi-Level Protection Scheme, the Data Security Law, and the Personal Information Protection Law. At the time of writing, amendments to update the CSL are being discussed, which could raise the maximum fine from one million yuan to fifty million.[227]

Insofar as personal data protection is concerned, the CSL improved the Chinese framework on several points, but remained far behind from the European Union's requirements. Even though the scope of the Chinese legislation was broader and therefore was converging more with the European approach of an omnibus data protection law (as expressed by the Convention 108 of the Council of Europe,[228] the 1995 Directive[229] and the GDPR),[230] than with the United States'method of data protection through many sectoral laws,[231] the protection granted to individuals remained limited. In addition, the CSL is vaguely worded, which makes it difficult to implement in practice. The vagueness of Chinese law is such by design, as the high-level binding law is supplemented by standards and guidelines, which are easier to modify and alter than it is to change a national law.[232] And, indeed, guidelines on personal data protection were published in 2018: the Personal Information Protection Specification (2018 Specification).[233]

[Cybersecurity Law of the People's Republic of China] (passed by the Standing Committee of the National People's Congress Nov. 7, 2016, effective June 1, 2017). Translation (unofficial) available at https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (last visited January 22, 2023) [hereinafter CSL].

[227] Xinmei Shen, *China Plans Steeper Fines to 'Frighten' Cybersecurity Offenders*, S. CHINA MORNING POST, Sep. 15, 2022, https://www.scmp.com/tech/policy/article/3192599/china-eyes-steeper-cybersecurity-fines-intimidate-offenders-big-tech (last visited Jan. 29, 2023).

[228] Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 10, 1985, ETS No. 108 (1985).

[229] 1995 Directive, *supra* note 119.

[230] For a distinction between the "European elements" in data protection law v. the "Global elements" that do not originate from the European approach, *see, e.g.*, *The Influence of European Data Privacy Standards Outside Europe*, *supra* note 218, at 73–74.

[231] Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: the Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 360 (2005).

[232] Creemers, *supra* note 217, at 4–5. ("This is no strange occurrence in the Chinese legal landscape: a law often only includes basic elements of principle, purpose, and punishment, mandating government departments and local departments to formulate more detailed implementing regulations and technical standards to provide detailed prohibitions, obligations, and procedures.").

[233] Xìnxī Ānquán Jìshù Gèrén Xìnxī Ānquán Guīfàn (信息安全技术个人信息安全规范) [Information Security Technology – Personal Information Security Specification - (GB/T 35273-2017)] (issued by the National Information Technology Standardization Technical

The most worrisome, and therefore the most noted, feature of the law for multinational companies was the requirement of data localization in certain circumstances. Article 37 of the CSL indeed mandates that critical information infrastructure operators store personal data and important data within mainland China. Given the lack of clear definitions at the time, companies transferring data fell into a grey area.[234] After several attempts, China recently clarified the extent of the localization requirement to some extent.[235]

It is in the 2018 Specification that the Chinese convergence with EU rules became the most visible. The scope was much broader than that of the CSL; more rights were granted, and principles and requirements were more stringent. However, they were only non-binding guidelines, even though they clearly showed the direction that China was taking.[236] This direction was later confirmed in binding law with the Personal Information Protection Law, discussed in Section 4. But, even though significant progress was made, the Chinese data protection framework remained lighter than what is expected by the EU's adequacy standards. In 2019, a new scheme was introduced to complement the CSL—the Multi-Level Protection Scheme. Article 21 of the CSL mandates network operator compliance with the Multi-Level Protection Scheme (MLPS). The MLPS ensures that the relevant cybersecurity practices are implemented, based on the risks associated with the considered technology systems. It is composed of several texts (first enacted before the CSL) and developed by the Ministry of Public Security (MPS),[237] with the latest major overhaul in 2019.[238]

At its core, MLPS is a set of five levels of security requirements for information systems, depending on their criticality. Level 1 is the lowest one and a self-assessment is sufficient, while level 5 is the highest one and the authorities are to be involved in the oversight and controls. Networks classified as level 2 and above are required to be audited and certified by a licensed firm.[239]

The MPS and the local Public Security Bureaus ensure the law's enforcement. Sanctions include fines and denial of a company's business

---

Committee (the TC260) on Dec. 29, 2017, effective May 1, 2018). Unofficial translation available at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/. A draft of a revised version was published in 2019.

[234] *See infra*, Part V.A.

[235] *See infra*, Part V.B.

[236] Daniel Albrecht, *Chinese First Personal Information Protection Law in Contrast to the European GDPR*, 23 COMPUTER L. REV. INT'L 1 (2022).

[237] Creemers, *supra* note 217, at 3.

[238] Jim Fitzsimmons, *Enforcement of China's Multi-Level Protection Scheme - The Rapid Roll-Out of Cyber Security Compliance*, Control Risks, https://www.controlrisks.com/campaigns/china-business/enforcement-of-chinas-multi-level-protection-scheme (last visited Nov. 15, 2023).

[239] Jim Fitzsimmons, *supra* note 235.

license renewal or the renewal conditioned on getting the MPLS certification.[240] The MLPS is more about cybersecurity than personal information protection *per se*, but it does reinforce data security overall and it lays the groundwork for the Data Security Law.[241]

2. Data Security Law (2021)

The Data Security Law (DSL)[242] has several State objectives, such as to support education and scientific research institutions, enterprises, and so on, to establish a categorized and graded protection system for data,[243] a data security emergency response mechanism and a data security review system.[244] Chapter V of the law is about data security protection obligations for the entities handling data based on the cybersecurity Multi-Level Protection System.[245] It also underlines the organizational and management obligations, as well as the need to follow the requirements of outbound data transfers which, for personal data, are guided by the Personal Information Protection Law and the related guidelines.

3. Personal Information Protection Law (2021)

The Personal Information Protection Law[246] from 2021 (PIPL) is at the pinnacle of the evolution of data privacy law in China. The Chinese approach gradually moved from a U.S.-like model with sectoral laws with minimal protection, to a more EU-resembling model with broad scope rules and stronger requirements, culminating in the CSL and its Personal Data Protection Specifications.[247] Those Specifications were a great leap forward and sign of convergence, but were not binding rules, leaving companies uncertain as to whether they were building their compliance on unstable grounds.

Fortunately, the PIPL was soon enacted and confirmed the direction identified previously, that is, China was converging with the European Union

---

[240] *Id*.

[241] Creemers, *supra* note 217, at 3.

[242] Zhōnghuá Rénmín Gònghéguó Shùjù Ānquán Fǎ (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (passed at the 29th meeting of the Standing Committee of the 13th National People's Congress on June 10, 2021, effective Sept. 1, 2021), [hereinafter DSL].

[243] *Id*. art. 20–21.

[244] *Id*. art. 23–24.

[245] *Id*. art. 27.

[246] Zhōnghuá Rénmín Gònghéguó Gèrén Xìnxī Bǎohù Fǎ (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] (passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on Aug. 20, 2021, effective Nov. 1, 2021), [hereinafter PIPL] Translation (unofficial) available at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[247] Pernot-Leplay, *supra* note 46.

more and more. PIPL indeed shows proximity with the GDPR in several ways. The fines for breaching the law are substantially increased. They can now go up to 50 million Yuan or 5 % of annual revenue, which is nearly as deterrent as GDPR fines (up to 20 million Euros or 4 % of annual revenue).[248] The extra-territorial jurisdiction, that is also a strong specificity of the GDPR,[249] is now also a feature of Chinese law, with even somewhat similar wording.[250] The lawful grounds for processing data are included in PIPL, and they have been expanded, as consent is not the only possible ground anymore. Like under the GDPR, it is now possible to handle data without specific consent from individuals if it is, among others, to conclude or fulfill a contract in which the individual is an interested party, to fulfill statutory duties, or to protect natural persons' lives and health.[251] However, there is no mention of the legitimate interest of the data controller (or handler), which is a legal basis often used under the GDPR. This means that many processing operations performed based on legitimate interests in Europe will need to rely on consent in China.

PIPL gives several rights to individuals, also found in the GDPR, including those which are required for an adequacy determination. Among the individual rights present in PIPL are the right to information and to object (refuse), right to access, data portability, right to rectification (correction or completion), and the right to be forgotten (or to deletion).[252] Prior to PIPL, the CSL provided fewer rights, as some were found only in the 2018 Specification which was not binding law. On the side of data handlers, China imposes a set of obligations that can also be found in the GDPR, such as performing an impact assessment for higher risk data processing,[253] additional safeguards for handling sensitive personal information,[254] and an obligation to notify authorities in case of data breach.[255] As discussed in Part V, China's rules on data exports also partly converge with EU requirements.

Overall, PIPL indeed represents a great coming together of Chinese rules with those of the GDPR. There are also significant differences however, which decisively bar the possibility of an adequacy decision from the Commission for China, and should be a prime focus when carrying out a TIA for China. In addition to these main laws on data protection and cybersecurity, related rules can be found in over thirty laws and sectoral regulations (including the Civil Code, the E-Commerce Law or the Criminal

---

[248] PIPL, *supra* note 246, art. 66.

[249] *See, e.g.*, GDPR, *supra* note 54, art. 3(2).

[250] PIPL, *supra* note 246, art. 3 (although PIPL adds a catchall phrase, allowing its application to processing activities outside of China, in "Other circumstances provided in laws or administrative regulations." *Id*. art. 3(3)).

[251] *Id*. art. 13.

[252] *Id*. art. 44–47.

[253] *Id*. art. 55.

[254] *Id*. arts. 28–32.

[255] *Id*. art. 57.

Law) and dozens of standards.[256]

One of the criteria for a Commission adequacy determination is having one or more independent data protection supervisory authorities.[257] China does not have an independent data protection authority in the European sense. The CSL gave a planning and coordinating role to the Cyberspace Administration of China (CAC), that the PIPL has confirmed,[258] which has been described by researchers as an opaque party-state entity.[259]

The CAC is the principal authority, but industry regulators also play a role in the enforcement of the rules, such as the Ministry of Industry and Information Technology for telecommunications and information technology, the China Insurance Regulatory Commission for the insurance industry, or the China Banking Regulatory Commission for the banking industry, in addition to the local Public Security Bureau branches. Over the last few years, the CAC has become a prominent actor of China's enforcement of data laws, beyond personal information protection, to the point of being called a "super-regulator" by observers.[260] The National Information Security Standardization Technical Committee (also known as TC260) is in charge of creating the multiple standards that are parts of China's cyberspace regulatory framework (more than 300 standards have been issued and 700 more are being drafted).[261] It is not an enforcement body, although the standards may be compulsory or just recommended. But, even for the latter, they are considered as "quasi-implementing rules"[262] and a "reference point"[263] for regulators, especially considering the common vagueness of binding laws discussed above.

Furthermore, the authorities that exist in China are "subordinated to the central government," and in that sense, are not independent, and their

---

[256] Hongquan (Samuel) Yang, *China*, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 115 (6th ed. 2022).

[257] GDPR, *supra* note 54, art. 45(2)(b).

[258] CSL, *supra* note 226, art. 8; PIPL, *supra* note 246, art. 60.

[259] Jamie P. Horsley, *Behind the Facade of China's Cyber Super-Regulator*, DIGICHINA (Aug. 8, 2022), https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/.

[260] *Id.*; AJ Caughey & Shen Lu, *How the CAC Became Chinese Tech's Biggest Nightmare*, PROTOCOL (Mar. 11, 2022), https://www.protocol.com/china/china-cac-tech-crackdown.

[261] Clara Wang, *Here's Who Has the Ear of China's Most Active Cyber Regulator*, PROTOCOL (Jan. 27, 2021), https://www.protocol.com/china/tc260-china-cyber-regulator-companies.

[262] Anna Gamvros, *China Data Privacy: New Guidance to Strengthen Protection of Personal Data*, NORTON ROSE FULBRIGHT (Mar. 2017), https://www.nortonrosefulbright.com/en/knowledge/publications/f5ca9809/china-data-privacy-new-guidance-to-strengthen-protection-of-personal-data.

[263] Yan Luo, *China's New Draft National Standards on Personal Information Protection*, COVINGTON (Jan. 6, 2017), https://www.insideprivacy.com/international/china/chinas-new-draft-national-standards-on-personal-information-protection/.

multiplicity leads to inconsistency and unpredictability.[264] Thus, this GDPR requirement for an adequacy determination appears not to be met. Next, this study turns to two additional issues that are crucial to an EU adequacy determination: rule of law and government access to data. The results of this analysis will form the basis for this study's provisional view on the mirage of "adequacy."

B. Rule of Law in China and Government Access to Data

For a data protection framework to be deemed essentially equivalent to that of the European Union, one crucial point is that it should provide protection from private actors but also from government access that does not respect the essence of their fundamental rights. The question is so sensitive that it remains a major issue today between the European Union and the United States, as demonstrated in Part III. Due to its specific political structure and context, limits on China's government access to data are notoriously frail and evanescent. The reasons come from the laws themselves but also and decisively from broader issues of rule of law in China.

Although Chinese and Western laws share similarities, it is essential in any comparative law study to recall the fundamental differences concerning the rule of law. During the past history of China, the concept of the rule of law did not reach the level of prestige it enjoys in the West.[265] Today, the Chinese Communist Party (Party) is the uncontestable leader of China. It is so stated in the Constitution itself, which proclaims in its first article that the People's Republic of China is a democratic dictatorship led by the Party.[266] Therefore, the Party and the state are structurally integrated, which creates an ambivalence towards the concept of rule of law.[267] Although governing according to the law has been stated and confirmed as a principle, most notably after the rebuilding of the legal system following the cultural revolution,[268] researchers underline the intertwined nature of the rule of law

---

[264] *See, e.g.*, Anja Geller, *How Comprehensive Is Chinese Data Protection Law? A Systemisation of Chinese Data Protection Law from a European Perspective*, 69 GRUR INT'L 1191, 1200 (2020).

[265] Matthieu Burnay, Joëlle Hivonnet & Kolja Raube, *Bridging the EU-China's Gap on the Rule of Law?*, 14 ASIA EUR. J. 95, 98 (2016) [hereinafter Burnay et al.] (The authors note that Confucius already favors moral principles over legal rules).

[266] Zhōnghuá Rénmín Gònghéguó Xiànfǎ (中华人民共和国宪法) [Constitution of People's Republic of China], XIANFA art. 1 (1982), *translated in Constitution of the People's Republic of China*, THE PEOPLE'S REPUBLIC OF CHINA (NOV. 20, 2019, 4:25 PM), http://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html.

[267] *See generally*, Ling Li, *"Rule of Law" in a Party-State: A Conceptual Interpretive Framework of the Constitutional Reality of China*, 2 ASIAN J.L. & SOC'Y 93 (2015) [hereinafter Li].

[268] Burnay et al., *supra* note 265, at 98–99.

and the rule of the Party in China,[269] and the "rule of law in a Chinese way."[270] The "Party-state controls both procedure and outcome in any court proceeding in which it takes an interest…."[271] As a result, although there is a theoretical separation of power, the Western definition of the rule of law, which is the first criterion for an adequacy determination listed in the GDPR,[272] is not effective in China in practice.[273]

Here, we can note that the U.S. system does not face similar issues, yet the lawfulness of data exports to the United States have regularly been challenged. At this point, the idea of an adequacy decision favorable to China can already be dismissed.[274] But, since data transfers often happen outside of an adequacy decision, for example through EU SCCs, a deeper understanding of this issue in China is in order.

Government access to personal data is one of the factors to be taken into account in determining adequacy (or not) of data protection under the GDPR, and its existence may go against the protection of human rights, which is similarly cited as a factor, after the rule of law.[275] In China, the fact that the legal framework expressly allows the government to access data for state and public security is well documented and may indicate a lack of adequate regard for human rights,[276] and, more relevantly, argues against an adequacy determination. Yet, with the emergence of personal information protection arose discussions about whether the government and public sector were restricted by the new rules. In theory, the broad wording of the CSL indeed

---

[269] Li, *supra* note 267.

[270] Weidong Ji, *The Rule of Law in a Chinese Way: Social Diversification and Reconstructing the System of Authority*, 1 ASIAN J.L. & SOC'Y 305 (2014); Li, *supra* note 267.

[271] Donald Clarke, *Order and Law in China*, 2022 U. ILL. L. REV. 541, 590 (2022).

[272] GDPR, *supra* note 54, art. 45(2)(a).

[273] Burnay et al., *supra* note 265, at 100.

[274] Speaking of recent additions to China's data protection legislative framework, one author comments that, "That does not mean, however, that it satisfies adequacy requirements under EU law, in particular in view of China's law enforcement problem, popular law breaches and the likely window-dressing of the Binding Corporate Rules." THE EU AS A GLOBAL DIGITAL Actor, *supra* note 24, at 183 (citation omitted).

[275] GDPR, *supra* note 54, art. 45(2)(a).

[276] Zhizheng Wang, *Systematic Government Access to Private-Sector Data in China*, *in* BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 241, 244 (Fred H. Cate & James X. Dempsey eds., 2017), https://doi.org/10.1093/oso/9780190685515.003.0011 (last visited Feb. 5, 2023) (Wang noted that the government "enjoys an extensive and unrestricted power of investigation and censorship of communications whenever state security or public security is involved). *See also* Polonca Kovač & Grega Rudolf, *Social Aspects of Democratic Safeguards in Privacy Rights: A Qualitative Study of the European Union and China*, 20 CENT. EUR. PUB. ADMIN. REV. 7, 24 (2022) ("If EU seems to dedicate a lot of attention to the proportionate balance of data protection on one side and (administrative) transparency on the other side, Chinese developments are rather unilateral in terms of more and more strict surveillance mechanisms of the state over its people.").

did not cast them out of its scope, although observers remained skeptical,[277] but the PIPL later did not exclude public organizations from its scope either. Its actual enforcement against State organs remains to be seen, but the means that PIPL gives to individuals go in the right direction.[278]

On the other hand, the CSL does mandate network operators to provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities.[279] A requirement with similar wording, although not limited to cyber issues, exists at Article 77 of the National Security Law of China.[280] The National Intelligence Law is perhaps the one that raises the most concerns, as it requires organizations and citizens to support and cooperate with China's national intelligence efforts.[281] Used in conjunction with data localization requirements in the CSL, this provides a powerful legal means for China to access data, including personal information, and represents a serious burden for foreign companies.[282] Because it also applies to Chinese subsidiaries in foreign countries,[283] it reinforces foreign concerns about their relation with Chinese authorities.[284] One of the latest examples is

---

[277] Graham Greenleaf & Scott Livingston, *China's New Cybersecurity Law – Also a Data Privacy Law?*, 144 PRIVACY L. & BUS. INT'L REP. 1, 3 (2016), https://papers.ssrn.com/abstract=2958658 (last visited Feb. 5, 2023) (Greenleaf however notes that this would be an "extraordinary new development.").

[278] Jamie P. Horsley, *How Will China's Privacy Law Apply to the Chinese State?*, BROOKINGS (Jan. 29, 2021), https://www.brookings.edu/articles/how-will-chinas-privacy-law-apply-to-the-chinese-state/ . Horsley, commenting on a late draft of the law, observes that PIPL's "requirements to all state organs reflects a largely aspirational intent at present, and it would maintain broad authority for state organs to access and use personal information to perform broad statutory functions."

[279] CSL, *supra* note 226, art. 28.

[280] That article "requires all citizens and organizations to make timely reports on activities that endanger national security, truthfully provide evidence relating to to such activities that one knows of, and provide the necessary support and assistance to national security agencies. If enforced strictly, the provision could be used to compel netizens to report 'harmful information' or activity in cyberspace, and throw China back to the days of the Cultural Revolution where everyone was under the constant surveillance of each other," although that has not been the case so far. Henry Gao, *Data Regulation with Chinese Characteristics*, *in* BIG DATA AND GLOBAL TRADE LAW 245, 251 (Mira Burri, ed., 2021).

[281] Zhōnghuá Rénmín Gònghéguó Guójiā Qíngbào Fǎ (中华人民共和国国家情报法) [National Intelligence Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong, June 27, 2017, effective June 28, 2017) (Revised April 27, 2018), art. 7, *translated in PRC National Intelligence Law*, CHINA LAW TRANSLATE (July 27, 2017), https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/?lang=en.

[282] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017, 11:30 AM), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[283] MANNHEIMER SWARTLING, APPLICABILITY OF CHINESE NATIONAL INTELLIGENCE LAW TO CHINESE AND NON-CHINESE ENTITIES 1 (2019), https://www.mannheimerswartling.se/app/uploads/2021/04/msa_nyhetsbrev_national-intelligencelaw_jan-19.pdf.

[284] Jan Czarnocki et al., Government Access to Data in Third Countries 18 (2021) [hereinafter Czarnocki et al]. As put by another author, "China … is generally mistrusted as a

the current examination of Alibaba Cloud for national security risks, especially related to the protection of personal information and intellectual property.[285]

Related to that, NGOs regularly alert on China's abuses on fundamental rights including data protection and privacy.[286] Western media report the expansive collection of personal data for security reasons in China through a system of mass surveillance.[287] Even though China denies these reports, they reinforce the foreign concerns about government access to data, without adequate protections for individuals.

Together with the CSL, DSL, and PIPL, China's data protection legal framework does provide individuals with rights and redress mechanisms. However, their effectiveness in practice, when it comes to remedies in case of access to personal information by law enforcement or intelligence agencies, has been questioned by reports and research.[288] Therefore, the questions around safeguards in the area of government access to data that plague the EU-U.S. data transfers are relevant for EU-China data flows as well. In sum, because of failings with respect to several GDPR adequacy criteria, government access to personal data and surveillance without EU-style procedural protections such as effective redress, and lack of respect for human rights and rule of law, this study's preliminary view is that a Commission adequacy determination for China is not envisageable at this time. However, as transfers of data occur otherwise through the use of adequate safeguards such as EU SCCs, this study now returns briefly to the issue of *Schrems II*-mandated TIAs.

With respect to the use of TIAs, in this context, one of the key elements will be how to face up to government surveillance. Supplemental measures from among those mentioned in Part III.E. will be required as the EEG test will not have been satisfied. This involves an analysis of whether or not certain technical and organizational measures may legally (and effectively) be used in China to block certain state access to data. Given the pre-eminent role of the state and the focus of legislation on protection against private

non-democratic country, and the recent adoption in 2017 of a new National Intelligence Law, obliging Chinese companies to collaborate with Chinese intelligence agencies, certainly does not help." Edoardo Celeste, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, *in* DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES N EXTRATERRITORIALITY AND SOVEREIGNTY 211, 219 (Federico Fabbrini, Edoard Celeste & John Quinn eds., 2021) (citation omitted).

[285] Alexandra Alper, *U.S. Examining Alibaba's Cloud Unit for National Security Risks*, REUTERS (Jan. 19, 2022), https://www.reuters.com/technology/exclusive-us-examining-alibabas-cloud-unit-national-security-risks-sources-2022-01-18/.

[286] *How Mass Surveillance Works in Xinjiang, China*, HUMAN RIGHTS WATCH (May 2, 2019), https://www.hrw.org/node/329492.

[287] Isabelle Qian et al., *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State*, N.Y. TIMES, (Jun. 21, 2022), https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html.

[288] *See, e.g.*, Czarnocki et al., *supra* note 284, at 19–21.

actors, rather than the state, the response may potentially be in the negative, in which case there may be a requirement to halt data transfers, although these are matters for data exporters, with cooperation from data importers, to determine.

C. Conclusion to Part IV

Data protection rules in China have made decisive progress in the recent years. Individuals enjoy many new rights, such as the rights to access, to rectify data, to be informed about the processing, and the rights to data portability and to be forgotten, which come from EU law. Although, to date, certain requirements remain vaguely worded, related guidelines and specifications are regularly drafted, submitted for public consultation and eventually published, similarly to what the EDPB does in Europe. The strengthening of Chinese data protection law is a process that will take time, but its direction towards more protection for individuals remains confirmed, to date. However, the oversight on government access to data and related redress mechanisms remain an issue. The Chinese paradox, whereby data protection laws become stricter, but government data access is hardly affected by them, persists. Because the same problem caused the invalidation of data agreements for EU-U.S. data transfers in the *Schrems I* and *Schrems II* cases, this Part IV shows that the same concerns are present in the case of China, with even more intensity. In this context, despite all of China's progress in data protection rules, a Commission adequacy decision seems out of the question, and TIAs carried out by companies for the purpose of EU SCCs, for example, should carefully consider these same issues, bearing in mind the *Schrems II* requirement that the importer must be able, in the context of Chinese law, regulation, and practice, to respect the terms of those EU SCCs.

V. CHINESE RULES ON DATA TRANSFERS: BEYOND SIMILARITIES WITH GDPR, THE MARK OF CHINA'S OWN APPROACH

The restrictions on data exports out of China are a crucial element to ensure both the protection of personal information and the national security. In addition to the government access to data highlighted in Part IV, rules pertaining to national security are present mainly in rules on cross-border data transfers and data localization. Discussing how China intertwines data privacy with national security will in turn allow to ponder the rationale behind China's own approach and its direction, which then may influence other jurisdictions and swarm to digital sovereignty, geopolitics, and ultimately, power.

Some of the most salient specificities of China's data protection law are thus found in its restrictions on cross-border data transfers, in particular the need to pass a security assessment and the overlap of data privacy and

national security. The study of such specificities is crucial given the importance of China in the globalized economy[289] where, for example, an EU or a U.S. firm may engage in foreign direct investment in that country[290] and need to export personal data back to their home office, such as HR data or customer data, much like flows from the European Union to the U.S. were a concern when the European Union first instituted data transfer restrictions in the 1995 Directive, prior to the GDPR.[291]

This Part handles these issues as follows: first, the building of a legal framework is detailed in Section A. Second, Section B sets out circumstances when data transfers are allowed, subject to conditions being met. Third, the distinct basis for Chinese data protection law, focusing on national security, is analyzed in Section C. Finally, concluding remarks regarding this Part are made in Section D.

A. The Building of a Legal Framework for Data Transfers

Rapidly emerging data laws in China cause compliance difficulties for foreign firms,[292] especially the rules on cross-border data transfers. Until the latest texts were established, requirements were much vaguer and left foreign companies facing hazard in navigating grey areas. It was challenging to understand if one could transfer data without restrictions, or if, at the complete opposite, they should process data in China only, due to assumed data localization requirements.[293]

---

[289] China, the world's second largest economy, is the largest goods trading partner of the United States, for example. *See* U.S.-China Trade Facts, *supra* note 55.

[290] This is the case for many companies as, for example, U.S. foreign direct investment in China in 2020 totaled $123.9 billion. *Id*.

[291] *See* OF PRIVACY AND POWER, supra note 2, at 130–31 (citing Ira Magaziner, then U.S. President Clinton's "e-commerce "czar," from a September 2000 interview, on the 1995 Directive and its data transfer restriction: "a lot of our companies were reacting with great concern, and coming to us in government and saying this is a nightmare, and it's going to affect our investments in Europe….[T]hey were facing a huge investment plus that there was a risk that the normal data that they needed to operate their business with subsidiary companies and so on, would be put in danger….They thought it was a potential disaster.").

[292] *See* Kandy Wong, *US firms say China's 'ambiguous' data laws are creating a 'uniquely restrictive' environment*, S. China Morning Post, Apr. 21, 2022, https://www.scmp.com/economy/china-economy/article/3174887/us-firms-say-chinas-ambiguous-data-laws-are-creating-uniquely; Chris Marquis, *How Western Companies Are Dealing with China's Data Security Laws*, CHINA PROJECT (June 1, 2022), https://thechinaproject.com/2022/06/01/how-western-companies-are-dealing-with-chinas-data-security-laws/.

[293] Yan Luo, Zhijing Yu & Vicky Liu, *The Future of Data Localization and Cross-Border Transfer in China: a Unified Framework or a Patchwork of Requirements?*, IAPP, June 22, 2021, https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/ ("It is important to note that the CSL, DSL and draft PIPL do not clarify how data localization requirements interact with cross-border transfer requirements. Additionally, these laws do not explain whether 'localization' only refers to the storage of data locally or if it extends to the localization of other processing activities. Thus, there remains an amount of uncertainty on how these

Provisions for cross-border data transfers are contained mainly in the CSL and PIPL. The CSL rules target both personal information and important data handled by critical information infrastructure operators (CIIOs), while PIPL focuses on personal information. As is common in China,[294] those binding laws are vague and need other lower-level texts to be practically applicable. The requirements of binding laws are therefore supplemented by implementing rules and guidelines. The debates that surround them and the different drafts that came out show the sensitivity of the topic of cross-border data transfers out of China.

Here, it is worth noticing that although restrictions on data transfers are often seen as directed against foreign businesses, they have also been interpreted as a "crackdown on Chinese tech,"[295] in a context where several actions against Chinese tech giants and their leaders had been taken.[296] However, while they do give authorities more power to act, the new rules are the result of developments that started before these events.[297] The CSL, in particular, caused many concerns within the business community, because of restrictions on data transfers that are both broad and strict.[298] Its Article 37 indeed states that "critical 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."[299] Businesses can provide it out of the territory only where "truly necessary," following a security assessment. But this type of assessment was not yet designed then, and certain crucial terms such as "critical information infrastructure operators" or "important data" lacked a clear definition.

At the time, certain elements resembling GDPR requirements (more stringent than OECD Guidelines or U.S. laws) could be identified from the

obligations will impact companies in practice.").

[294] Dong Han, *From Vagueness to Clarity? Articulating Legal Criteria of Digital Content Regulation in China*, 12 GLOBAL MEDIA & COMM. 211 (2016). Han argues that the vagueness of Chinese law is due to China's political and ideological ambiguity towards the development of the Internet. *See also* Creemers, *supra* note 217, at 5.

[295] Samm Sacks et al., *Knowns and Unknowns About China's New Draft Cross-Border Data Rules*, DIGICHINA (Nov. 5, 2021), https://digichina.stanford.edu/work/knowns-and-unknowns-about-chinas-new-draft-cross-border-data-rules/ [hereinafter Sacks et al.].

[296] Billy Perrigo, *Here's What to Know About China's Sweeping Tech Crackdown*, TIME (Sep. 1, 2021), https://time.com/6094156/china-big-tech-regulation-us/; Sam Peach, *Why Did Alibaba's Jack Ma Disappear for Three Months?*, BBC NEWS (Mar. 20, 2021), https://www.bbc.com/news/technology-56448688.

[297] Sacks et al., *supra* note 295; Jinhe Liu, *China's Data Localization*, 13 CHINESE J. COMM. 84, 87 (2020) [hereinafter Liu].

[298] *China Adopts Cybersecurity Law Despite Foreign Opposition*, BLOOMBERG.COM, (Nov. 7, 2016) https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition; Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, HENRY M. JACKSON SCH. INT'L STUD. (Feb. 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

[299] CSL, *supra* note 226, art. 37.

guidelines on personal data accompanying the CSL.[300] However, those similarities were more with respect to other areas of data protection and less on cross-border data transfers. There, parallelism stopped at the principle of restrictions on data exports, which is typical of EU law, rather than U.S. law.[301] Beyond that, what started to show at the time was the inception of China's own approach to the regulation of data flows, embodied by the concept of cyber-sovereignty established by the CSL in its first article,[302] and the inclusion of "important data" into the restrictions.

Despite the concerns expressed by observers and businesses, the CSL became effective as such. The CAC subsequently published two different drafts about cross-border data transfers, but neither was finalized,[303] and the application of those rules was even postponed.[304] The situation changed following the DSL and PIPL coming into effect in 2021.[305] The PIPL, in particular, mentioned three distinct means to transfer data out of China: passing a security assessment, being certified, or relying on contractual clauses.[306] The CAC issued the final version on the security assessment on July 7, 2022, which eventually became effective on September 1, 2022: the Outbound Data Transfer Security Assessment Measures (Assessment Measures).[307] The Assessment Measures are formulated based on the CSL, DSL and PIPL,[308] and therefore concern both *personal* data and *important*

---

[300] *See generally*, Pernot-Leplay, *supra* note 46, at 78 and 91–103.

[301] Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn To Institutions and Procedures*, 126 HARV. L. REV. 1966, 1977 (2013) (Describing this difference between the EU and U.S. models as a "dramatic distinction."). For a discussion of U.S. law's position on data transfers, *see* Part II. For a discussion of EU data transfer restrictions, *see* Part III.

[302] This concept of cyber sovereignty is central to data governance in China and is achieved through "asserting national jurisdiction over the Internet." *The Beijing Effect*, *supra* note 38, at 24. The cyberspace becomes subordinated to the interests and values of a country within its borders, i.e. the application of state sovereignty to cyberspace, *see* Pernot-Leplay, *supra* note 46, 103–106 for the consequences of the concept on data transfer rules, and, *generally*, Rogier Creemers, *China's Conception of Cyber Sovereignty*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 107 (2020).

[303] Sacks et al., *supra* note 295.

[304] Yuan Yang, *Trade War with US Delays China's Rules Curbing Data Transfers*, FIN. TIMES (Apr. 21, 2019), https://www.ft.com/content/c8f4b066-60df-11e9-b285-3acd5d43599e.

[305] Attentive observation of the PIPL drafting shows that, among the stated objectives of this law, "safeguarding the flow of personal data lawfully, orderly and freely" was removed between the first and the second draft, which demonstrates the will to restrict personal data flows while enhancing security. *See* Guan Zheng, *Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China*, 43 COMPUTER L. & SEC. REV. 105610, 9 (2021) [hereinafter Zheng].

[306] PIPL, *supra* note 246, art. 38.

[307] Shùjù Chūjìng Ānquán Pínggū Bànfǎ (数据出境安全评估办法) [Outbound Data Transfer Security Assessment Measures] (published by the CAC, July 7, 2022, effective Sept. 1, 2022), *translated in* Outbound Data Transfer Security Assessment Measures Translatio available at [hereinafter Assessment Measures]. [hereinafter Assessment Measures].

[308] *Id*. art. 1.

data together. Just prior to the Assessment Measures, on June 24, 2022, the TC260 released Technical Specifications for the Certification of Cross-Border Processing of Personal Information (Certification Specifications), about the certification system for cross-border data transfers among entities of a same group (akin to EU BCRs).[309] Then, on June 30, 2022, the CAC published the draft Standard Contract Provisions for Exporting Personal Information Abroad (draft Standard Contract Provisions), which is a means to export data similar to the EU SCCs under the GDPR.[310] The final version came shortly after, on February 24, 2023, to come into force on June 1, 2023,[311] with little substantial difference from the draft.[312]

Fortunately, the final version of the Assessment Measures now defines the term "important data," although its first draft lacked that crucial definition.[313] All three texts provide many useful and long-awaited details and procedure for transferring data out of China, outlining the numerous conditions for doing so. The security assessment is the mean to export data most specific to China. The certification and contractual clauses are more

---

[309] Wǎngluò Ānquán Biāozhǔn Shíjiàn Zhǐnán—Gèrén Xìnxī Kuà Jìng Chǔlǐ Huódòng Ānquán Rènzhèng Guīfàn (网络安全标准实践指南—个人信息跨境处理活动安全认证规范) [Practice Guidelines for Cyber Security Standards—Security Certification Specifications for Cross-Border Processing of Personal Information] (published by TC260, June 24, 2022, draft version), https://www.tc260.org.cn/upload/2022-06-24/1656064151109035148.pdf [hereinafter Certification Specifications]. The TC260 then released a substantially similar draft for public comment on March 16, 2023 (https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381).

[310] 54 Guójiā Hùliánwǎng Xìnxī Bàngōngshì Guānyú "Gèrén Xìnxī Chūjìng Biāozhǔn Hétóng Guiding (Zhēngqiú Yìjiàn Gǎo)" (国家互联网信息办公室关于《个人信息出境标准合同规定（征求意见稿）》) [The National Internet Information Office's "Standard Provisions on Personal Information Export Standard Contracts (Draft for Comment)"] (published by the CAC, June 30, 2022, draft version), http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm [hereinafter Draft Standard Contract Provisions]. For a listing of the transfer tools (or, appropriate safeguards) under the GDPR, including the EU SCCs, *see* Part III.C.

[311] Gèrén Xìnxī Chūjìng Biāozhǔn Hétóng Bànfǎ (个人信息出境标准合同办法) [Measures for Standard Contracts for Exporting Personal Information Abroad] (published by the CAC, February 24, 2023, effective June 1, 2023), http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm (in Chinese).

[312] Yan Luo Liu Nicholas Shepherd, Xuezi Dan, *China Finalizes Standard Contract for Cross-Border Transfers of Personal Information*, INSIDE PRIVACY (Feb. 24, 2023), https://www.insideprivacy.com/international/china/china-finalizes-standard-contract-for-cross-border-transfers-of-personal-information/.

[313] Guójiā Hùliánwǎng Xìnxī Bàngōngshì Guānyú "Gèrén Xìnxī Hé Zhòngyào Shùjù Chūjìng Ānquán Pínggū Fāngfǎ (Zhēngqiú Yìjiàn Gǎo)" (国家互联网信息办公室关于《个人信息和重要数据处境安全评估办法（征求意见稿）》）[The National Internet Information Office's "Outbound Data Transfer Security Assessment Measures (Draft for Comment)"] (published by the CAC, April 11, 2017, draft version), http://www.cac.gov.cn/2017-04/11/c_1120785691.htm (in Chinese). Translation available at https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/

familiar to foreign companies as they follow the EU approach (although not entirely).

B. Data Transfers Allowed Subject to Conditions

As mentioned above, under PIPL personal information can be transferred abroad when data handlers "truly need" to do so, in several circumstances mentioned above: passing a security assessment; having obtained a relevant certification; concluding a contract with the foreign receiving side; or any other mechanism as prescribed by laws, administrative regulations, or the CAC.[314] Another circumstance relates to potential other conditions provided by other laws and regulations, and a last possibility refers to treaties and international agreements under which cross-border transfers would be allowed – those may come to exist in the future, but have not been entered into, as yet.

Personal data cannot be exported on the request of a foreign law authority unless Chinese authorities approve such action.[315] This relates to several concerns about the extraterritorial reach of foreign laws, such as the U.S. Cloud Act.[316] That Act has been the topic of heated debates within the data privacy community, such as whether the Cloud Act is even applicable in the European Union,[317] and the compliance difficulties that it inevitably raises.[318] In China, PIPL gives a clear answer, but the dilemma exists, and some companies may face a legal conundrum.

It is important to note that, under PIPL, data transfers can only occur when individuals have been properly informed and provide separate consent[319] – even though PIPL provides more legal grounds for data processing outside of transfers. This could create a significant compliance burden for data handlers. In the European Union, the GDPR provides bases for exporting data even without individuals' consent, such as, for example,

---

[314] PIPL, *supra* note 246, art. 38.

[315] *Id*. art. 41.

[316] Clarifying Lawful Overseas Use of Data Act § 103, 18 U.S.C. §§ 2703, 2713.

[317] *See, e.g.*, *Annex: Initial Legal Assessment of the Impact of the US CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence* (July 10, 2019), https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en. For a short discussion of this, *see Obstacles to Transatlantic Harmonization*, *supra* note 51, at 430–31.

[318] *See* Matthias Artzt & Walter Delacruz, *How to Comply with Both the GDPR and the CLOUD Act*, IAPP (Jan. 29, 2019), https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/; *See also* Peter Church & Caitlin Potratz Metcalf, *U.S. CLOUD Act and GDPR – Is the Cloud Still Safe?*, LINKLATERS (Sept. 13, 2019), https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe.

[319] PIPL, *supra* note 246, art. 39 ("Where personal information handlers provide personal information outside of the borders of the People's Republic of China, they shall notify the individual . . . and obtain individuals' separate consent.").

the necessity for the performance of a contract.[320] However, the 2021 draft on Online Data Security Management Regulations (draft Data Security Regulations)[321] provides for an exception where data is transferred "as required for concluding or fulfilling a contract where an individual is a concerned party, or personal information is provided abroad as necessary for protecting individuals' lives or health, or the security of their property."[322] As this text is currently only a draft, the matter should be followed closely.

Finally, another limitation that is not often discussed is the possibility that PIPL gives to China to forbid all data transfers to a certain jurisdiction as retaliation against prohibitive or restrictive measures against China.[323] Here is where geopolitical power could come to play. For example, if the European Union were to limit data transfers to China because it considers China not to provide an adequate level of data protection,[324] China could adopt reciprocal measures.

Now, this Section turns to three "tools" that may be used to help allow for data transfers. First, China's version of the EU BCRs—Certifications for Data Transfers—is studied. Then, EU SCCs are compared with China's standard contractual clauses, prior to discussing China's Outbound Data Transfer Security Assessment Measures.

1. Certification for Data Transfers: The Chinese Version of the GDPR's BCRs

The PIPL certification scheme is sometimes compared to the EU BCR mechanism[325] under the GDPR.[326] Like them, certification is not mandatory and data exporters can decide to rather legitimize their data transfers through other ways such as the security assessment – which above certain thresholds becomes an obligation.[327] Unlike the EU BCRs however, the Chinese version

---

[320] GDPR, *supra* note 54, art. 49.1(b).

[321] Guójiā hùliánwǎng xìnxī bàngōngshì guānyú "wǎngluò shùjù ānquán guǎnlǐ tiáolì (zhēngqiú yìjiàn gǎo)" (国家互联网信息办公室关于《网络数据安全管理条例（征求意见稿）》) [Online Data Security Management Regulations (Draft for Comment)] (published by the CAC, November 14th, 2021, draft version). Translation available at https://digichina.stanford.edu/work/translation-online-data-security-management-regulations-draft-for-comment-nov-2021/.

[322] *Id*. art. 35.

[323] PIPL, *supra* note 246, art. 43 ("Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt reciprocal measures against said country or region on the basis of actual circumstances.").

[324] Zheng, *supra* note 305, at 11.

[325] GDPR, *supra* note 54, art. 47

[326] Samuel Yang, Christopher Fung & Leann Wu, *Will China's New Certification Rules Be a Popular Legal Path for Outbound Data Transfers?*, IAPP (Aug. 16, 2022), https://iapp.org/news/a/will-chinas-new-certification-rules-be-a-popular-legal-path-for-outbound-data-transfers/ [hereinafter Yang, Fung & Wu].

[327] *See infra* Part V.B.3.

does not need to be approved by the supervisory authority before data handlers can use it.[328]

This certification system is applicable to "transfers of personal information between multinational companies or subsidiaries or affiliated companies of the same economic or business entity," and to data handlers that are not based in China but nonetheless subject to PIPL.[329] The Certification Specifications detail the list of elements that need to be specified in the legally binding and enforceable agreement between the data handler and the entity receiving the data, such as, among others, their identities, the purpose for the transfer, measures to protect individuals' rights and interests, and so on.[330] The agreement should specify the methods used to enforce individuals' rights and effectively how to allow them to be exercised, such as how individuals may access their data, lodge a complaint, correct or delete their data, or not be subject to decisions based solely on automated decision-making.[331]

Many of these requirements will be familiar to entities subjects to the GDPR. There are also organizational obligations, for example about data protection officers or the need to conduct Personal Information Protection Impact Assessments (PIPIA) prior to sending data abroad (which repeats PIPL's requirement to perform a PIPIA when data is transferred abroad in Article 55(4)). Such requirements will not be foreign to those entities either, and they can certainly rely on many of the practices and culture they built for GDPR compliance.

Unfortunately, as they are today, the Certification Specifications are not well enough defined to allow companies to rely confidently on them for their data transfers. Indeed, the certification institutions are not specified, although it is likely that the CAC will designate at least the China Cybersecurity Review Technology and Certification Center and the China Electronics Standardization Institution.[332] Without official designations of those authorities, the Certification Specifications are not fully actionable. The validity period for the certification and what would trigger the need to update have not yet been specified either. Additionally, the personal information impact assessment that should be conducted before a transfer must feature an analysis of the "legal environment" and the "network security environment," but what is required here is left unclear.[333]

In Europe, EU BCRs are not a popular way of handling data transfers,

---

[328] Amigo L. Xie et al., *What You Need to Know About China 'Binding Corporate Rules' Under the New Certification Specifications*, NAT'L L. REV. (July 22, 2022), https://www.natlawreview.com/article/what-you-need-to-know-about-china-binding-corporate-rules-under-new-certification [hereinafter Xie et al.].

[329] Certification Specifications, *supra* note 309, art. 1.

[330] *Id*. art. 4.1.

[331] *Id*. art. 5.1.

[332] Xie et al., *supra* note 328.

[333] Yang, Fung & Wu, *supra* note 326.

notably because it is a long and costly process for companies.[334] New guidance and clarification for their Chinese counterparts are awaited, but they are foreseen as a more costly solution than using contractual clauses.[335] Presently, it seems unlikely that certification under PIPL will be a mainstream solution for data transfers.

2. Standard Contract Provisions: PIPL v. GDPR

Under the GDPR, Standard Contractual Clauses (EU SCCs) are a popular means to transfer data outside of the EU, provided that a contract between the exporter and the recipient is in place and contains those binding EU SCCs. Under PIPL, the first draft of China's standard contractual provisions (Standard Contractual Provisions, or China SCCs) was published on June 30, 2022, and the final version on February 24, 2023.[336]

The Standard Contract Provisions clarify when data handlers may use them for transferring data. This is namely when the following conditions are met: (i) the data handlers are non-critical infrastructure information operators; (ii) they handle personal information of less than a million people; (iii) they have exported the data of less than 100,000 people since the first of January of the previous year; and (iv) the cumulative number of data subjects whose sensitive personal information was provided overseas has not reached 10,000 people, during the same period.[337] Crossing these thresholds would trigger the need to pass the state-conducted security assessment, discussed in Section 3. There is no mention of the concept of "important data," a Chinese characteristic in data protection law. This gap has been pointed out by observers and practitioners for the draft version,[338] and was unfortunately not clarified in the finalized version, but a new proposal could bring more clarity on the matter.[339] Also, the thresholds mentioned above are a first significant difference from the EU SCCs, which are available to all data controllers, in contrast to China SCCs.

Like for certification, data handlers are required to conduct PIPIAs before sending data abroad.[340] Each PIPIA must include assessments on (i) the legality, legitimacy, and necessity of the purpose, scope, and method of processing data; (ii) the quantity, scope, type, and sensitivity of personal information exported abroad and associated risks; (iii) the responsibilities

---

[334] Alexandra Ross & Volha Samasiuk, *BCRs: 'Best Case Route' or 'Better Call Reinforcements'?*, IAPP (Nov. 27, 2018), https://iapp.org/news/a/bcrs-best-case-route-or-better-call-reinforcements/ (last visited Dec. 27, 2022).

[335] Yang, Fung, and Wu, *supra* note 324.

[336] See *supra* notes 307–308.

[337] Draft Standard Contract Provisions, *supra* note 310, art. 4.

[338] Michael Tan, Julian Sun & Kyle Tong, *China: SCCs and Their Implementation*, TAYLORWESSING (Aug. 16, 2022), https://www.taylorwessing.com/en/insights-and-events/insights/2022/08/china-sccs-and-their-implementation.

[339] See *infra* Part V.B.3.

[340] Draft Standard Contract Provisions, *supra* note 310, art. 5.

and obligations promised by the overseas receiving party, along with organizational and technical measures to fulfill those responsibilities; (iv) the risks of data breach (leakage, tampering, abuse, etc.); and (v) the impact of policies and regulations of the jurisdiction where the data are sent. If there is a change in the data protection legal framework of the recipient country, new SCCs should be signed between the parties; such renewal will also be necessary if there is a change in the purpose, scope, type, sensitivity, quantity, method, storage period, storage location of personal information provided overseas, or "other circumstances that may affect the rights and interests of personal information."[341] Finally, the standard contract and the accompanying PIPIA shall be filed with the local provincial network information department within ten working days following the effective date of the contract.[342]

Now that China has adopted the EU practice of standard contractual clauses, the issue of potential conflicts between the two systems can legitimately be raised. Given the extensive use of EU SCCs in practice, law firms and practitioners have already proposed comparisons between EU SCCs and their Chinese counterparts (for the draft).[343] First, China SCCs form a single set of clauses, and do not distinguish transfers controller to controller, controller to processor, and so on, in the EU manner. Other differences relate to a notification obligation, stricter obligations for onward transfers, or the more restrictive approach to providing information to foreign authorities.[344]

3. Outbound Data Transfer Security Assessment Measures (Assessment Measures): A Chinese Characteristic, Often Mandatory

As introduced, the Assessment Measures were released to provide details to the PIPL requirement on the security assessment.[345] In addition to them, on August 31, 2022 (one day prior to the entry into force of the Assessment Measures), the CAC issued guidance specifying practical details of the requirements related to the assessment (the Guidelines).[346] This

---

[341] *Id.* art. 8.

[342] *Id.* art. 7.

[343] Samuel Yang & Chris Fung, *Cross-Border Data Transfers: A Comparison of the EU and Chinese Standard Contractual Clauses.*, ANJIE BROAD (July 11, 2022), https://www.chinalawvision.com/2022/07/intellectual-property/cybersecurity/cross-border-data-transfers-a-comparison-of-the-eu-and-chinese-standard-contractual-clauses/ [hereinafter Yang & Fung]; Yan Luo et al., *How China's Draft SCCs Compare with EU SCCs*, IAPP (July 21, 2022), https://iapp.org/news/a/how-chinas-draft-sccs-compare-with-eu-sccs/ [hereinafter Luo et al.]; Graham Greenleaf, *China's Standard Contractual Clauses: Restricted Use and Complex Terms*, 178 PRIV. L. & BUS. INT'L REP. 1, 6–7 (July 12, 2022).

[344] Yang & Fung, *supra* note 343; Luo et al., *supra* note 343.

[345] Assessment Measures, *supra* note 307, art. 2. Those Measures are also relevant for the export of "important data" by CIIOs, as Article 37 of the CSL refers to the security assessment and these rules which were yet to be enacted when the CSL came to effect.

[346] Shùjù Chūjìng Ānquán Pínggū Shēnbào Zhǐnán (Dì Yī Bǎn) (Data Export Security

mechanism is likely to be often used in practice, because the threshold requiring it will put many multinational companies in its scope. It is also a specificity of Chinese law, because unlike the certification system and China's SCCs, there is no counterpart to this mechanism in the GDPR. At the time of writing these lines, the mechanism is very recent, but several security assessments have started, the first approvals have been reported,[347] and refusals have also been communicated to the authors. Overall, these restrictions have fostered significant concerns for foreign companies, which in turn could hurt China's post-pandemic economic recovery.[348] A proposal to lighten some of the requirements was published on September 28, 2023, and is discussed in this section.[349]

The Assessment Measures mandate for a state-conducted security assessment in the following circumstances:

1. Where the data handler provides important data abroad;

2. Critical information infrastructure operators and data handlers handling the personal information of over 1 million people providing personal information abroad;

3. Data handlers providing abroad the personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people since January 1 of the previous year;

4. Other circumstances where the State cybersecurity and informatization department provides data export security assessment must be applied for.[350] Before this security assessment, Article 5 of the Assessment Measures mandates personal information handlers to first perform a self-assessment (a form of PIPIA substantially similar to the one prescribed before relying on China SCCs); with a focus on data transfer issues such as contract clauses for the responsibility of the data importer, a catch-all requirement to

Assessment Declaration Guidelines (First Edition)) [数据出境安全评估申报指南（第一版）] (published by the CAC, Aug. 31, 2022, entered into force Sept. 1, 2022), http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm.

[347] Justina Zhang, *First Cases of Security Assessment Approval for Outbound Data Transfers in China*, GLOB. ADVERT. LAWS. ALL. (Feb. 20, 2023), http://blog.galalaw.com/post/102i7e2/update-first-cases-of-security-assessment-approval-for-outbound-data-transfers-i.

[348] Ryan McMorrow, *China Looks to Relax Cross-Border Data Security Controls*, FIN. TIMES (Sept. 28, 2023), https://www.ft.com/content/b1f9a792-1abe-4ca1-9818-b2b8ad266029.

[349] Guójiā HùliánWǎng Xìnxī Bàngōngshì Guānyú "Guīfàn Hé Cùjìn Shùjù Kuà Jìng Liúdòng Guīdìng (Zhēngqiú Yìjiàn Gǎo)" Gōngkāi Zhēngqiú Yìjiàn De Tōngzhī (国家互联网信息办公室关于《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见的通知) [Notice of the Cyberspace Administration of China on the Regulations on T)] (published by the CAC, September 28th, 2023) [hereinafter Proposal for Promoting CBDT].

[350] Assessment Measures, *supra* note 307, art. 4.

> assess "other matters that may influence the security of data provision abroad," but also an evaluation of the risks for national security and public interest. The Guidelines provide a template for this self-assessment.

If the security assessment is successful, the authorization is valid for two years, but data handlers need to re-apply if changes happen related, for example, to the purpose, category of data transferred, cybersecurity environment in the target jurisdiction, or changes in control power of the receiving party.[351] Certain observers raise a point of uncertainty as to the time that the assessment would take, especially considering the involvement of local provincial-level cybersecurity and informatization department.[352] However, specific deadlines are prescribed in the text for both the provincial-level review and the subsequent state-level review. First, Article 7 mandates provincial-level cybersecurity and informatization departments to communicate to data handlers within five working days whether their application is complete; if it is, then they have seven working days to decide if it is accepted or not. Then, national cybersecurity and informatization departments has forty-five days to complete the assessment, although this deadline may indeed be extended at the CAC's discretion. In total, a security assessment could take up to fifty-seven working days if there is no extension required.[353] Practice will tell if authorities comply with these timeframes.

Under the draft proposal, which was open to public comments until October 15, 2023, certain data processing activities would be exempted from reviews, certification or standard contractual clauses, which would greatly alleviate the compliance burden for many companies. The targeted processing can be very common and do not, themselves, raise concerns for China's national security, such as academic cooperation, marketing, cross-border shopping or flight reservation.[354] Importantly, transfers necessary for human resources management is included in the list. Another significant change that this proposal would bring, if passed, is that data would be deemed important data only if publicly classified as such by one of the competent Chinese authorities.[355] This would greatly clarify all the uncertainties for multinational companies, which often had to assess without clear guidelines on whether their data are *important data* under Chinese law, and decide to accept or not the risks associated to it. Finally, the thresholds would be heightened and transfers of personal data of less than 10,000 individuals would not be subject to China's restrictions, and relying on standard

---

[351] *Id.* art. 14.

[352] Derek Ho & Mandy Zhu, *China Cross-Border Data Transfer Mechanism and its Implications*, IAPP (Aug. 23, 2022), https://iapp.org/news/a/china-cross-border-data-transfer-mechanism-and-its-implications/.

[353] Assessment Measures, *supra* note 307, art. 12.

[354] Proposal for Promoting CBDT, *supra* note 349, art. 1.

[355] *Id.* art. 2.

contractual clauses would be possible until the data of one million persons is transferred outside of China.[356] Without changing the underlying rationale supporting Chinese rules, those potential new rules would facilitate the operation of international companies to a greater extent than under current rules. No precise date for the finalization of those rules have been stated.

C. Data Protection with Chinese Characteristics: Connection Between the Protection of Personal Data and National Security

In the EU, the protection of personal information is strong because it is a fundamental right. Whereas, in China, protecting personal data is necessary to safeguard national, economic, and political security and stability. This approach is being discussed at least since the CSL, sometimes against formal opposition from foreign countries, but the Chinese opinion is that data exports framework should consider national strategic concerns.[357]

The relationship between national security and data privacy is clearly underlined by Hong Yanqing, a Chinese scholar who led the drafting of technical standards on personal information protection:

> the huge amount of user information held by Alibaba, currently covering over 400 million users, is certainly personal information […] but because of its scale and granularity, it can also match the public security organs' basic national population database and even surpass it in accuracy. For the country, any eventual leak or damage of this scale of basic population data could create a serious threat to national security.[358]

The Assessment Measures are formulated to "regulate outbound data transfer activities, protect personal information rights and interests, safeguard national security and the social public interest, and promote the secure and free cross-border flow of data."[359] The intertwining of the need to safeguard the protection of both personal information and national security is specific to China (as are the requirements in PIPL targeting critical information infrastructure operators) and does not exist in GDPR. In Europe, the two issues are addressed separately, with clearer distinctions. This is enshrined in Article 8 of the Assessment Measures, requiring the assessment of "the risks that outbound data transfer activities may bring to national security, the public interest, and the lawful rights and interests of individuals and

---

[356] *Id.* art. 5–6.

[357] Creemers, *supra* note 217, at 5. For a discussion about China's rationale on data localization rules specifically, *see* Liu, *supra* note 297, at 98. (As the author concludes, "China views data localization as political security protection from foreign hostile forces, and they assume that there are short-term industrial benefits. More importantly, as the basic resource of high-tech development, data are regarded as the key element. The construction of a data dam meets the three needs of security, economy, and technology.").

[358] Creemers, *supra* note 217, at 4.

[359] Assessment Measures, *supra* note 307, art. 1.

organizations."[360]

To understand the applicability of this assessment, there are terms that crucially need to be defined. The first circumstance pertains to data handlers exporting "important data." Both the CSL[361] and DSL[362] require important data handlers to pass a security assessment to be allowed to export such data. But the meaning of "important data" has long been a topic of speculation and concerns, due to the vagueness and lack of clear definition of the term in Chinese rules.[363] The Assessment Measures now state that they are data that, if "altered, destroyed, leaked, illegally acquired or illegally used, etc., may harm national security, economic operations, social stability, public health or security, etc."[364] This definition does not exclude personal information from being qualified as important data; in fact, *sensitive data* under PIPL may be deemed *important data* as well, the risk should be properly assessed on a case-by-case basis.

The second circumstance concerns CIIOs, who must, by default, store personal data within China. But PIPL does not define what is a CIIO, a term first introduced in the CSL with a description but waiting for further specification.[365] The meaning can now be found in the Critical Information Infrastructure Security Protection Regulations [366] from 2021. Its Article 2 specifies that CIIOs are in the following sectors: public communications and information services; energy; transportation; water conservancy; finance; public services; e-government; defense technology industry; plus "other important network facilities and information systems that, once damaged, disabled or suffer a data disclosure, may severely threaten the national

---

[360] *Id*. art. 8.

[361] CSL, *supra* note 226, art. 37.

[362] DSL, *supra* note 242, art. 31.

[363] Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect; Yanqing Hong, *The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources* (June 20, 2017) (working paper found at https://law.yale.edu/yls-today/news/china-center-paper-details-cross-border-data-regime-cybersecurity-law). Hong, who led the drafting of data protection standards for the TC260, attempted to clear the confusion and explained that "[t]o sum it up in one sentence, the introduction of the concept of 'important data' in essence serves the objective need to protect national security and public interests in the big data era, and on the national level it is a natural response to the particularities of data security protection in the big data era." However, the above-mentioned new proposed rules could bring more clarity on the matter, see *supra* Part V.B.3.

[364] Assessment Measures, *supra* note 307, art. 19.

[365] CSL, *supra* note 226, art. 31.

[366] Guānjiàn Xìnxī Jīchǔ Shèshī Ānquán Bǎohù Tiáolì (关键信息基础设施安全保护条例) [Critical Information Infrastructure Security Protection Regulations] (passed by the 133rd Standing Committee meeting of the State Council, Aug. 17, 2021, effective Sept.1, 2021), https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.

security, national economy, people's livelihood or public interest."[367] Therefore, China cyber laws regulate CIIOs not only from the network security perspective, but also from a data privacy standpoint; like the focus on national security, this characterizes China's approach. In Europe, those actors and sectors are targeted in regulations focused on cybersecurity such as the NIS[368] and NIS 2[369] Directives, but not specifically in personal data protection rules.

The third circumstance relates to sensitive data. Sensitive data are specifically protected in both the EU and China, but they aren't defined in the same way. While GDPR provides an exhaustive list comprising health, sexual orientation, or religion, and so on,[370] PIPL choses a risk-based approach.[371] As discussed above, sensitive data could also be considered important data in some cases. Overall, these rules mean that data handlers will first have to determine and explain if and why they process personal information and/or important data (which entails dedicated risk assessments) and if they belong to the CIIOs category.

D. Illustration of Impacts on U.S. and Chinese Firms

To avoid complications and the overall uncertainty of Chinese rules on data transfers, several multinational companies have decided to store their data in China. Apple was, and still is, abundantly criticized in the media for storing locals' data within China's mainland at a state-owned company's data centers.[372] And Tesla announced it will store locally all data collected from

---

[367] For each of these sectors, it belongs to the competent industry regulators to draw up the rules for determination of CIIO.

[368] Directive 2016/1148 of the European Parliament and the Council Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, O.J. (L 194) 1 (July 19, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. For a discussion about the relationship of the NIS Directive and the GDPR, *see generally*, Dimitra Markopoulou, Vagelis Papakonstantinou & Paul de Hert, *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, 35 COMPUTER L. & SEC. REV. 105336 (2019).

[369] Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, O.J. (L 333) 80 (Dec. 27, 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN.

[370] GDPR, *supra* note 54, art. 9.

[371] PIPL, supra note 246, art. 28 ("Sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.").

[372] Jack Nicas, Raymond Zhong & Daisuke Wakabayashi, *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. TIMES (May 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html; Paul Mozur, Daisuke Wakabayashi & Nick Wingfield, *Apple Opening Data Center in China to*

cars sold in China, following governmental concerns around the use of sensitive data (such as location and images from cars' cameras) for reasons of privacy as well as national security, which led to a ban of Tesla cars for military personnel.[373] Logically, avoiding the need to transfer data abroad alleviates or even suppresses the compliance risks attached to it. Where not required to comply with data localization under the CSL, for example, these actions could be classified as soft data localization.

Finally, recent cases decisively show the interplay between data privacy and national security. In July 2022, the CAC fined the ride-hailing app Didi RMB 8 billion (US $1.2 billion) for violating laws on data security and personal data protection.[374] Although the details have not been revealed officially, it's been reported that risks on overseas data transfers were among the main causes for the sanction, the issue here was the collection and other processing of location data and travel information of important individuals.[375]

E. Conclusion to Part V

The continuance of China's convergence with the European Union on several rules is a significant example of a legal transplantation for comparative law scholars. However, what is perhaps the most novel and non-obvious is deciphering China's own direction on data protection and especially cross-border data transfers. This topic that is indeed a vivid concern for countless foreign companies, as well as part of the discussions around digital sovereignty and the geopolitics of data.

What characterizes China's voice on data localization is certainly its broad scope, which partly comes from vague definitions or even their lack thereof, leaving business in grey areas of legal uncertainty. Another Chinese characteristic that can be observed when comparing China's approach with the European Union's, is the conjunction between privacy and national security. The first issue is partly being improved by the new guidelines and standards that came out since the enactment of PIPL. It is an ongoing work and much remains to be sorted out, as illustrated by the draft rules recently released, proposing to alleviate certain requirements and could decrease the need to rely on CAC's security assessment. On the other hand, the tight interplay between personal data protection and national security is likely to

Comply With Cybersecurity Law, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html.

[373] Trefor Moss, *Tesla to Store China Data Locally in New Data Center*, WALL ST. J. (May 26, 2021), https://www.wsj.com/articles/tesla-to-store-china-data-locally-in-new-data-center-11622015001; Michelle Toh, *Tesla Sets up Data Center in China Amid Spying Concerns*, CNN (May 26, 2021, 3:58 AM), https://www.cnn.com/2021/05/26/business/tesla-china-data-center-intl-hnk/index.html.

[374] Eva Dou, *China Fines Didi $1.2 Billion for Breaking Data-Security Laws*, WASH. POST (July 21, 2022), https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/.

[375] *Id.*

remain a characteristic of Chinese law, whereas the U.S. and the EU each chose to rather primarily focus on one to regulate cross-border personal data transfers.

Both contractual clauses and the certification system are concepts transplanted from the GDPR. There are specificities to China's versions, but nothing too unfamiliar for foreign companies. New legal texts to make these systems applicable in practice are expected to be passed soon. However, Chinese law features another specificity, the security assessment, which is bound to become an essential way to transfer data out of the country. Its particularity is to focus the assessment on the risks that data transfers may pose to national security, public interest, and the rights of individuals. The recent example of the large fine against Didi is a sign that personal data, especially when sensitive or in a large amount, could indeed raise concerns for national security. Researchers and practitioners should remain attentive to future cases and observe the confirmation of this trend, and its intensity.

VI. CONCLUSION

Data may be a source of government power in terms of national security and competitiveness. As a result, today personal data protection is the object of geopolitics, and the three main power blocs covered by this study—the United States, the European Union, and China—all have different strategic objectives, which influence their choice of the nature of regulation of personal data. The United States, which historically built its self-regulatory system in a way that encouraged the development of U.S. big tech that is centered in Silicon Valley, has chosen a neoliberal policy. The European Union, which considers data protection as a fundamental right, places the focus on protecting an individual's rights with respect to the processing of his or her personal data. In addition, the extraterritorial effect of EU data protection legislation may be seen to level the regulatory playing field with U.S. and Chinese big tech. Finally, China's view on data protection is closely linked to national security, social control and power, with government access to data as an important characteristic.

These different data protection cultures are reflected in the way that each bloc has chosen to regulate data flows—at the heart of this study which concerns flows both into and out of China. Although not largely covered previously in the literature, and certainly not in the same holistic fashion, data transfer regulation into and out of China has become of great interest today because of a dawning era of Chinese big tech. Recent and existing regulation may be seen on a spectrum with the United States described as light touch, the European Union as prescriptive with conditional transfer, and China as being categorized into the restrictive or guarded approach, with transfer restrictions under PIPL and other regulation and data localization under the CSL. In each case, strategic goals are furthered by the choice of regulation.

However, this picture is neither black nor white, as this study has shown.

While the United States promotes free flow of data around the world, when U.S. individual privacy has been affected by certain Chinese or Chinese-controlled firms, the United States has taken regulatory or executive action to prohibit transfers and effectively encourage what might be called soft data localization. This has occurred in a period of obvious tension between China and the United States. Yet, the adoption of U.S. federal data privacy legislation, under consideration in the U.S. legislature today, may be one way to provide the legal tools necessary to control certain data flows, without resort to case-by-case executive orders, although this is a matter for future study. While the few cases cited in this article do not indicate a systemic change yet, and U.S. limitation of transfers is nothing like the data transfer restrictions of either of the other two blocs, continuing tensions may change this. One question this study leaves open, then, is will the United States lean more to a EU-style prescriptive approach with conditional transfers, or will it balance more toward a Chinese-style national security model, or neither of the two?

The European Union's position is based on established law, which in today's GDPR, is merely an evolution of the 1995 Directive adopted twenty-nine years ago. It sets out relatively clear criteria for obtaining an adequacy determination, allowing the free flow of data between the European Union and the "adequate" importing nation. However, today China does not benefit from such a determination and does not enjoy the same geopolitical position with respect to Europe as the United States does, which allowed that nation to benefit from the Safe Harbor and the Privacy Shield data agreements in the past and now from the EU-U.S. Data Privacy Framework data agreement. Thus, adequate safeguards must be used to allow for personal data flows from the European Union to China, and these may be conditioned on the use of supplemental measures, as well.

A preliminary analysis by this study of the prospects of an eventual Commission adequacy determination leads to a negative answer, even if China's PIPL features characteristics from the GDPR. Furthermore, some aspects of China's data protection laws and regulation cause concern for the use of adequate safeguards such as EU SCCs to transfer data to China without supplemental measures and, even then, if the importer could comply with those clauses in the face of the Chinese government's right to access data, presumably without the necessary procedural protections that a *Schrems II* transfer assessment would require. In the meantime, EU regulators may be more watchful of Chinese firms in this new age of Chinese big tech.

With respect to outgoing flows from China, this study has shown that, while data transfer regulations have not been finally fleshed out with interpretative guidance, they should be seen to be subject to considerations of national strategic concerns. The security assessment, mandatory for many data transfers, intertwine data protection and national security. In addition, CSL's data localization requirements have broad scope and limit the ability to export personal data when they apply.

In conclusion, it is likely that data flows into and out of China will continue to be subject to regulatory restraints, which may be amplified by actions in the United States, and that this situation is likely to endure over time. Geopolitical goals of the three power blocs reviewed in this study are varying and have led to different regulatory approaches to data transfers. Of course, as this study has shown, these regulatory approaches are also linked to different forms of power sought by the blocs. However, these impact the rights of individuals and economic activities of businesses, who will have to navigate these different regulations.