SciencesPo

CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

What specific measures could the US, the EU and China take in order to foster and facilitate cross-border data flows?

Veronica Arroyo, Karin Hess

Nicole Grünbaum & Gustavo Ribeiro

Comparative Approach to Big Tech Regulation (Spring 2023)

Professor Florence G'sell

April 2023

Table of contents

LIST OF ABBREVIATIONS

Abbreviation	Definition
APIs	Application Programming Interfaces
BCRs	Binding Corporate Rules
CAC	Cyberspace Administration of China
CCP	Chinese Communist Party
CCPA	California Consumer Privacy Act
CFIUS	Committee on Foreign Investment in the US
CISA	Cybersecurity & Infrastructure Security Agency
CLGISI	Central Leading Group for Internet Security and Informatization
CJEU	Court of Justice of the European Union
COPPR	Children's Online Privacy Protection Rule
CSL	Cybersecurity Law
DFI	Declaration on the Future of the Internet
DLR	Data Localization Requirement
DSL	Data Security Law
EDPB	European Data Protection Board
EU	European Union
EO	Executive Order
FISA	Foreign Intelligence Surveillance Act
FTA	Freedom Trade Agreement
FTC	Federal Trade Commission
FTZ	Free Trade Zone
GDPR	General Data Protection Regulation

HIPAA	Health Insurance Portability and Accountability Act
PETs	Privacy-Enhancing Technologies
PIPL	Personal Information Protection Law
PRC	People's Republic of China
RCEP	Regional Comprehensive Economic Partnership
SCCs	Standard contractual clauses
SIGINT	Signals intelligence
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
US	United States
USTR	Office of the United States Trade Representative

Abstract

This policy brief is addressed to the G20 Digital Economy Ministers and tackles the primary question: **what specific measures could the US, the European Union and China take in order to foster and facilitate cross-border data flows?** For this, it explores the principles and rationales that influence the regulation of data flows, and discusses the instruments that allow for data to flow across the People's Republic of China's, the European Union's and the United States of America's borders.

In doing so, it finds convergent and divergent points. The EU and the US have limited overlaps in regulation of data protection and privacy. Moreover, both polities diverge from China when it comes to national security, as the latter has legal means to restrict cross-border data flows on security grounds. The trade of digital goods and services is a priority for all three polities alike.

This policy brief advises the G20 Digital Economy Ministers to **adopt stabilizing measures** such as repositories, standards, and standard contractual clauses, and **explore transformative measures** including privacy-enhancing technologies, legally adequate data hubs in free trade zones, and a court with transnational jurisdiction.

Introduction

In an increasingly digital world, data has become a strategic asset for businesses, governments, and organizations. Firms are progressively relying on data to improve their operations, gain more efficiency and enhance users' experience (The Economist, 2017), while governments are also striving to create public value through data-driven public policies (OECD, 2019; OECD, 2014).

Global value chains, in which processes are fragmented, are also being transformed by data. Not only goods and services flow within these global production chains, but data is also inevitably exchanged. As Casalini et al. (2021) stress, "it is increasingly difficult for an international trade transaction to take place without a cross-border data transfer of some sort" (p.6). Data transfers become vital for organizations, both for their internal business functions and for their interactions with suppliers, providers and customers. Hence, cross-border data flows raise concerns about privacy, security, and data protection, among others. In the last two decades, governments have been responding to these trends and a patchwork of regulations, legal frameworks and agreements have resulted in a difficult landscape for firms and governments to navigate.

On the one hand, the European Union's (EU) market power coupled with its General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) has led it to become a global pioneer in data regulation (Bradford, 2020). Internally, the European Commission has launched A European strategy for data (European Commission, 2020) with the aim "to realize the vision for a genuine single market for data" (p.11). On the other hand, the United States (US) "takes a decentralized market-driven approach to its digital strategy" (OECD, 2017, p. 34). Indeed, it still lacks a federal framework, but strong citizen pressure has led to State level regulations, most notably those in California, Colorado, Connecticut, Virginia and Utah (Desai, 2023). A third major, but often overlooked, player in framing the international scene on data regulation is the People's Republic of China (PRC). In the past five years, the PRC has introduced a number of new regulations, including the Cybersecurity Law (CSL), the Personal Information Protection Law (PIPL), the Data Security Law (DSL), and the latest Measures for Cross-border Data Transfer Security Assessment, with the goal to establish a centrally controlled data governance framework.

The debate on the role of data usage and data transfers is unquestionably urgent, contemporary and relevant as "rule-making on data flows is hard to separate from geopolitical rivalry" (WEF, 2023). Indeed, "[t]he ownership and control of data flows have become a primary domain of US-Chinese competition for economic and geopolitical superiority" (Torreblanca, 2021, p.43). Likewise, the Digital Trade Restrictiveness Index reveals "that many leading economies put significant restrictions

on digital trade" (Ferracane et al., 2018, p.4). Moreover, in recent months, the Chinese app TikTok has been caught up in a US-China battle over its use of data (Criddle et al., 2023), and some European countries have prohibited its government officials from using it (Le Monde, 2023). As firms try to operate within the different regulatory frameworks set up by the triad of powers, governments continue to respond to an ever evolving scenario. In particular, China's newly established framework limits cross-border flows on the basis of public interest and national security concerns and, hence, takes an increasingly more restrictive regulatory approach.

In light of these new regulatory developments, and considering the commitment of the G20 Digital Economy Ministers to "work towards identifying commonalities, complementarities, and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust" (G20 Indonesia, 2022) this policy brief examines the following research question: what specific measures could the US, the European Union and China take in order to foster and facilitate cross-border data flows?

This report aims to i) clarify the regulatory fragmentation that has emerged in relation to cross-border data flows, ii) assess what is at stake for each of the three polities, iii) identify convergences as well as divergences, and iv) provide recommendations on actions that the G20 Digital Economy Working Group can consider in order to facilitate cross-border data flows.

For that aim, the report is structured as follows. The remainder of Section 1 introduces and forwards relevant definitions. Section 2 overviews each polity's framework for data governance coupled with effects to cross-border data flows. Section 3 draws convergences and divergences among each polity in three areas of policy that influence cross-border data flows. Section 4 tailors recommendations to the G20 Digital Economy Working Group based on the foregoing findings. Section 5 concludes.

1.1. Definitions

1.1.1. Cross-border data flows and data governance

The notion of 'cross-border data flows' refers to the "movement or transfer of information between computer servers across national borders" (Fefer, 2020, p.3). Key industries for economic growth heavily rely on cross-border data flows, including information services, high-value manufacturing, financial services, and e-commerce, just to name a few. According to McKinsey's latest study, "flows of data reached all-time highs" (Brishan et al, 2022) during and after the COVID-19 pandemic and grew at nearly 50 percent annually since 2010. A specific industry such as cross-border e-commerce has, according to WEF (2023), multiplied 45-fold in a decade to an estimated $2.7 trillion.

The concept of cross-border data flows is intrinsically linked to the notion of data governance. Data governance is defined as "the organization and implementation of policies, procedures, structure, roles, and responsibilities which outline and enforce rules of engagement, decision rights, and accountabilities for the effective management of information assets" (Ladley, 2012, p.11). Although definitions may slightly differ, data governance presumes the implementation of specific policies by an authority (governments, firms, or organizations) to ensure the adequate management of its data assets. The regulation of cross-border data flows, thus, falls within the data governance framework. As seen through the report, this conceptualization significantly impacts the actions taken by each polity[1].

1.1.2. Classification of data

One key issue related to data regulation is the challenging task of classifying it. As the OECD notes, "data is sometimes treated as a monolithic entity" (2020, p.12) but, in reality, it is heterogeneous. The EU, US and China define data in different ways, but as shown in Figure 1, overlaps may be found. Understanding how each polity defines and classifies different types of data is critical when trying to interpret the governance frameworks.

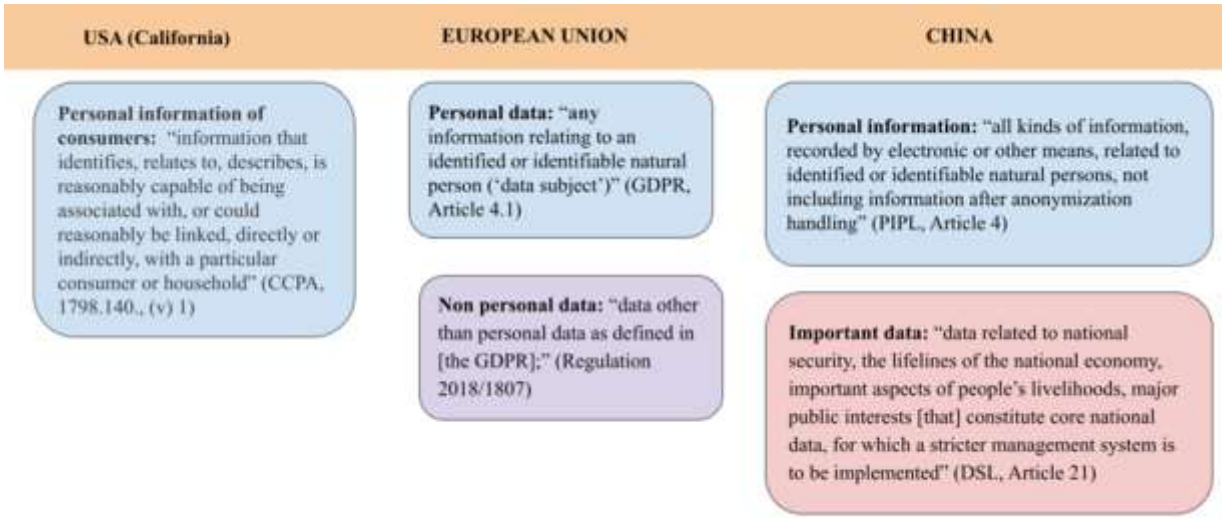


Figure 1: Definitions and classifications of data in the EU, US and China. Source: prepared by authors.

[1] And even broader, complex and multidimensional concept is the notion of cybersecurity. As Craigen et al. (2014) highlight, the term "is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative" (p.13). The US's CISA defines it as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information". The EU's Cybersecurity Act (2019) defines it as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" (Art. 2.1). Finally, China's Cybersecurity Law understands it as a means to "to prevent cyber attacks, intrusions, interference, destruction, and unlawful use, as well as unexpected accidents, to place networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential, and usable. (Art. 76).

Other approaches to data classification provide more nuances that could facilitate the convergence of governance frameworks. ISO's classification (ISO/IEC 20889:2018), for example, proposes a spectrum of data including identified data, pseudonymised data, unlinked pseudonymised data, anonymised data and aggregated data. As the OECD notes, this granularity can "help assess the level of risk to privacy and confidentiality, which in turn can help determine the degree to which legal and technical protection may be necessary, including the level of access control required" (2020, p.14).

1.2. Regulatory fragmentation

1.2.1. Why do countries regulate cross-border data flows?

The economic and social benefits of cross-border data flows are extensively documented. The European Center for International Political Economy explains that they help businesses reach foreign markets, better access digital suppliers and increase consumers' welfare by providing greater value for money and a wider variety of digital products (Ferracane et al., 2018, p.6). Nevertheless, countries are increasingly, but fragmentarily, regulating them. Many concerns are involved, including individual privacy and data protection, national security, issues related to intellectual property rights, "regulatory reach, competition policy and industrial policy" (Casalini et al, 2021, p.4).

International organizations and fora have tried to address the challenges of this regulatory proliferation and fragmentation, but competing priorities have hindered the task[2]. The OECD has provided some clarity on this topic, and released two reports, "Mapping Approaches to Data and Data Flows" (2020) and "Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers" (Casalini et al, 2021), with the aim to identify common elements in the regulatory instruments "that may serve as building blocks in bridging different approaches" (p.3). This exercise was a significant first step, but the situation calls for an in-depth search on what values and principles are at stake for each polity. This could ease the way towards greater interoperability and reduced regulatory fragmentation.

[2] Difficulties in reaching consensus have risen in high-level discussions, most notably in the G20 Digital Economy Working Group context. Lack of clarity and consensus resulted in a duplication of terms, i.e. "Data Free Flow with Trust and Cross-Border Data Flows" in the Ministerial Declarations. Moreover, in 2022, the Indonesian Presidency aimed to operationalize the concepts and to agree on "principles", but Ministers merely noted "the discussion initiated by the Indonesian G20 Presidency on lawfulness, fairness, and transparency in the context of its proposed 'principles' for data free flow with trust and cross-border data flows" (G20 Indonesia, 2022).

1.2.2. How do countries regulate cross-border data flows?

Depending on their policy objectives, preferences and type of data in question, countries have developed different regulatory approaches to cross-border flows that may be categorized in four ways.

On one end of the spectrum, some countries have no regulation on data transfers and, thus, data can be sent abroad with no restrictions. Others impose ex post accountability measures for the data exporter "if data sent abroad is misused" (Casalini et al., 2021, p.9), but no ex ante requirement is established. A stricter approach implies conditional flows on safeguards, which include "a range of preauthorized and transparent conditions for data transfer" (Casalini et al., p.9). The conditions vary, but usually refer to the adequacy or equivalence of the country where data is being transferred. In the cases where "the adequacy determination has not yet been made, firms can move data under options such as binding corporate rules, or model or approved contractual clauses" (p.9). Finally, the most restrictive countries only allow for case-by-case evaluation and ad hoc authorizations.

Besides these four broad categories, data localization requirements can also affect cross-border data flows, as a prohibition on data transfer requires that, consequently, data is processed and stored locally. Figure 2 provides examples on each case.

Figure 2: Approaches to data flows regulation. Source: prepared by the authors based on Casalini et al. (2021)

Based on these broad frameworks, a proliferation of instruments can be identified (see Table 1), in particular, i) unilateral mechanisms, ii) plurilateral arrangements, iii) trade agreements and partnerships, and iv) standards and technology-driven initiatives.

INSTRUMENT	DESCRIPTION	TOOLS & EXAMPLES
Unilateral mechanisms	Domestic tools that enable data transfers abroad if certain conditions are met	- Open safeguards: *ex post* accountability principles, contracts or private sector-led adequacy decisions - Pre-authorized safeguards: public adequacy decisions and public sector-led *ex ante* safeguards - Standard Contractual Clauses - Binding Corporate Rules
Plurilateral arrangements	International instruments that create rules around cross-border transfers of specific types of data, often on the basis of alignment on underlying principles	- Convention 108 of the Council of Europe - African Union Convention on Cyber Security and Personal Data Protection → usually occur in the context of personal data protection and privacy → enforcement depends on whether they are binding
Trade agreements	Contractual arrangement between countries concerning their trade relationships. They can incorporate provisions on data transfers.	- United States - Mexico - Canada Agreement - Framework Agreement on China-ASEAN Comprehensive Economic Cooperation - EU- MERCOSUR
Standards and technology-driven initiatives	Initiatives from private or non-governmental organizations	- ISO standards

Table 1: instruments that regulate cross-border data flows. Source: authors' production based on Casalini et al. (2021)

Although the landscape is complex and varied, some scholars envision a "clear global trend towards increasing convergence" (Şimşek, 2021). In this sense, identifying what values and principles are prioritized by each polity could be the next step to transcend the mapping of common instruments to the identification of possible principle-based convergences.

2. What is at stake for each polity?

This section overviews pieces of regulation, political strategies, and acts that glimpse at the interests each actor seeks to promote and safeguard in the context of cross-border data transfers, such as national security, free trade and privacy.

2.1. China

"There is no national security without cybersecurity" (没有网络安全没有国家安全) said Xi Jinping, General secretary of the Chinese Communist Party (CCP) and president of the PRC in the 2022 National Cybersecurity Awareness Week (People's Daily, 2022). This summarizes the two rationales China has as a regulator: domestically to maintain control and oversight over all kinds of data - be it industrial, financial, personal etc. - and internationally to build up a security governance framework that allows, above all, for safeguarding national security. The Chinese state believes that data-enabled means, such as cross-border data flows, could pose great harm to its national interests and, thus, enacts regulation accordingly. By limiting the cross-border flows of specific data types, China moves towards an increasingly more restrictive and case-by-case

regulatory approach. Yet, under the premise to uphold trade for economic growth, it simultaneously experiments with free cross-border transfer pilot zones and transfer-enabling provisions in Free Trade Agreements (FTA).

2.2.1 China's data governance framework

Since 2016, data governance has entered the status of paramount importance. That year, the first legislation in China's evolving cybersecurity framework was enacted, the "中华人民共和国网络安全法" (Cybersecurity Law, CSL). This legislation is overseen by the Central Leading Group for Internet Security and Informatization (CLGISI), a body in charge of policy formulation that reports to the highest organs in the CCP and/or the state apparatus, notably the Politburo Standing Committee, and the State Council (Chan, 2018). This double reporting to the Party and the State reflects the parallelism in the PRC's governing system and further shows the importance given to digital and data governance. China's primary cyber regulator is the Cyberspace Administration of China (CAC) which operates under the aforementioned CLGISI. Additionally, this year the National People's Congress (NPC) adopted a series of reforms including the establishment of a National Data Bureau to centrally manage data resources across the country (People's Daily, 2023).

The CSL can be summarized as legislation to defend national security and the rights of Chinese citizens within the PRC and abroad, as seen in Article 1: "ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests [...]" (NPC, 2016). For such, the legislation aims to differentiate between "Critical" and "Non-critical" information infrastructure operators. "Critical information infrastructure" is defined as: "if destroyed, suffering a loss of function, or experiencing leakage of data which might seriously endanger national security, national welfare, the people's livelihood, or the public interest" (Art. 31). Thus, the former has to "comply with outbound security management regarding the handling of important data" (Art. 37). CSL does not specify what type of data this terminology entails, leaving the specification to subsequent legislation.

More clarification on data protection yield two new laws that came into effect in the year 2021, the "中华人民共和国数据安全法" (Data Security Law, DSL) and the "中华人民共和国个人信息保护法" (Personal Information Protection Law, PIPL). The DSL defines important data (重要数据) as "data related to national security, the lifelines of the national economy, important aspects of people's livelihoods, major public interests, etc.", and that they "constitute core national data, for which a stricter management system is to be implemented" (NPC, 2021a, Art. 21). Moreover, regional departments should have autonomy in defining the scope of important data, and list them in a catalog.

The PIPL (2021) outlines personal information (个人信息) in Article 4 as "all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling" (NPC, 2021b), which is analogous to the definition used in the GDPR. Although enforcement may come to differ, normatively, the PIPL regulates processing by large technology companies, such as Tencent or Alibaba, and state organs alike; with some specificities and exceptions for the latter, as laid down in Section 3 (Horsley, 2021).

The DSL (2021), on the other hand, attempts to prevent harm to national security and public interest inflicted through data-enabled means, including cross-border data flows. Such a categorization of important data, which may encompass personal information, is according to leading scholars in the field a considerable innovation (Creemers, 2022). An example of this was the controversy around the New York-listed Chinese ride-hailing service Didi Chuxing "滴滴出行" which was used to access sensitive ministry locations. The Chinese regulators intervened in Didi's business operations out of fear that this data could be leaked to US authorities (Xinhua, 2021). Consequently, the Chinese government sees a strong need to regulate, as the transfer of important data to foreign actors is seen as a potential national security threat.

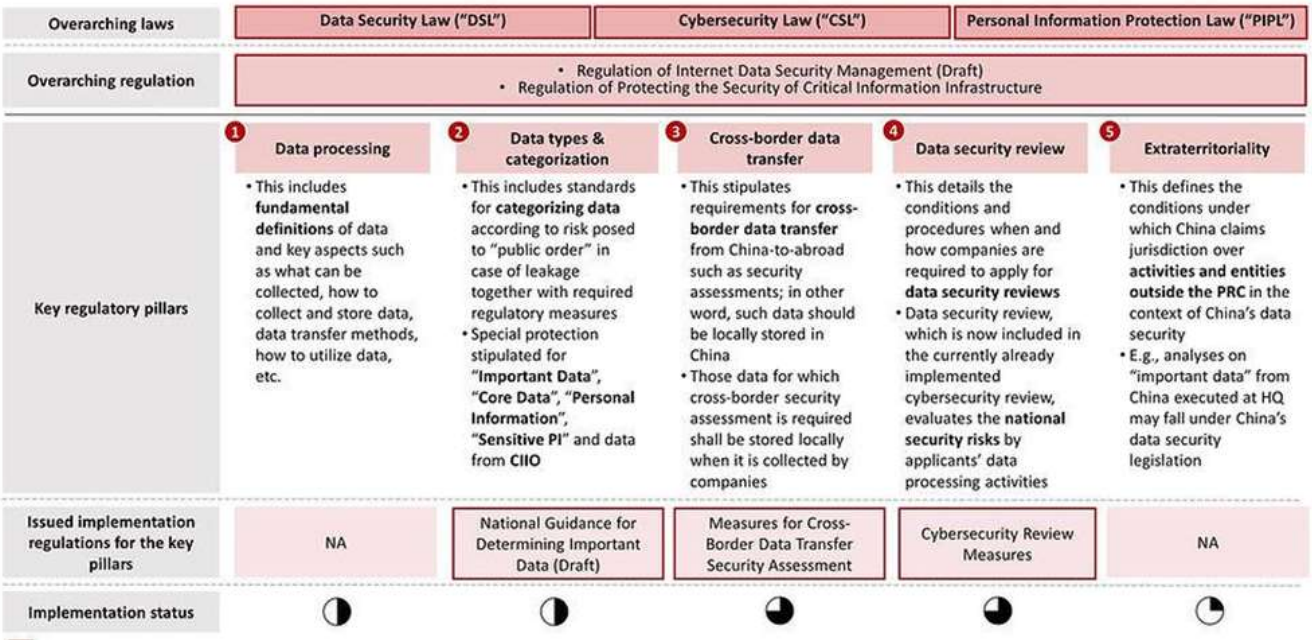


Figure 3 - Illustration of the PRC's data governance framework. Source: China Macro Group (2022)

2.2.2. Specific rules for cross-border data flows

On the question of data flows, the DSL Article 11 stresses that the State should promote the secure flow of important data across borders (出境安全管理), meaning that security measures are to be applied if important data is to be transferred outside of the PRC (Art. 21). Similarly, the PIPL sets provisions in Chapter 3 on how personal information

is to be handled in cross-border transfers. According to Article 38, the transfering party has to: “pass a security assessment, undergo personal information protection certification, conclude a contract with the foreign receiving side” or could benefit “from other conditions”, which are not further specified.

The Chinese data security governance framework should be understood as an evolving structure. Thus, the “数据出境安全评估办法” (Measures for Cross-border Data Transfer Security Assessment, the Measures), enacted in June 2022 (CAC), serves as another puzzle piece to specify terminology and procedure. Effectively, the Measures ask from companies who collect or produce through operations "important data" (Art. 19) or "personal information" - defined in quantitative terms as (i) personal information on over 100,000 people or (ii) sensitive personal information on over 10,000 people - a substantive security assessment if they want to provide this data abroad.

Table 2 summarizes the steps and the matching descriptions of the security assessment as outlined in Article 5 of the Measures.

Steps	Description
1. Conduction of outbound data transfer risk assessment	Data handlers - includes collection, storage, use, alteration, transmission, provision, disclosure, deletion, etc. (NPC, 2021b) - have to conduct an outbound data transfer risk assessment, e.g. how these transfers may engender national security and public interest.
2. Submission of application for security assessment	The application to the national cybersecurity and informatization department is submitted through the provincial-level department.
3. Legal documentation	Data handlers have to conclude a legal document about the purpose, limitations on scope/time as well as remedial measures with the foreign receiving party (Art. 9).

4. Conduction of security assessment	If the application is accepted, the national cybersecurity and informatization department entrusts a third-Party to conduct the security assessment (within 45 working days).
5. Next steps	Depending on the outcome, data handlers may re-apply for security assessment within 15 working days. If successful, they will benefit from "free" data flows for two years.

Table 2: China's security assessment. Source: authors' production based on Measures (CAC, 2022)

Given the very recent enactment of the Security Assessment Measures, there is little precedent on enforcement. However, in January 2023, a joint cancer treatment study between researchers from Amsterdam and Beijing was the first project to pass the security screening (Zhou et al., 2023). Nonetheless, most European companies take a conservative approach in either localizing their data or prevailing in "wait and see mode", as many terms of the Measures remain unspecific (Arcesati, 2022).

Until now, the PRC has signed 17 FTAs, yet, only six of them include e-commerce provisions (MOFCOM, 2023). Noteworthily, the FTA signed in 2015 with South Korea entails in its guidelines for subsequent negotiation a provision for the "transfer of information" (Annex 22A). Moreover, the Regional Comprehensive Economic Partnership (RCEP) stipulates the prohibitive norms on data localization (Art.12.14; 12.15), however, simultaneously allows for exception clauses (RCEP, 2020). Both hint at a future trend to include cross-border data flows in FTA negotiations and upgrades. This is enabled within China's regulatory framework. For instance, the PIPL (NPC, 2021b) states in its Article 38 that if treaties and international agreements "[...] contain relevant provisions such as conditions on providing personal data outside the borders of [the PRC], those provisions may be carried out [...]".

Moreover, China is piloting free cross-border data flows in selected free trade zones (FTZ), hence, testing grounds in which different policies and regulations are allowed in order to promote economic growth. For instance, Hainan island FTZ is set out to become an international hub for cross-border data flows under the oversight of president Xi (Hainan Government, 2023).

2.2. European Union

The EU places great importance on data protection as a fundamental right (Art. 8, Charter of Fundamental Rights). Yet, this is balanced with the "free movement of goods, persons, services and capital" internally (Art. 26, TFEU) and its pursuance of "free and fair trade" externally (Art. 3(5), TEU). Thus, it opts for a stricter approach to data flows.

2.2.1. The European Union's data governance framework

The creation of the European Union brought opportunities and challenges. It allowed its member states to constitute an internal market with free movement of goods, services, capital and persons (Treaty on the European Union, 2007, Article 3(3)). Being the largest single market, the EU has become an international actor in trade and portrays itself as “the world's largest trading bloc” (European Commission, n.d.). So far, the EU is the top trading partner for 80 countries, and has signed numerous trade agreements with third countries around the world (European Commision, n.d.).

Nevertheless, these projects have created challenges to fundamental rights and freedoms, especially the right to privacy (Charter of Fundamental Rights of the European Union, 2012, Art. 7), and personal data protection (Art. 8). The importance of having control over information concerning people is not new in the EU. It dates back to 1978, when Germany enacted the first Federal Data Protection Act (Bundesdatenschutzgesetz — BDSG) and established basic principles of data protection, such as the requirement of the data subject’s consent for personal data processing.

Therefore, there is a need to balance the rights and freedoms concerning those informational goods and the promotion of the internal market.

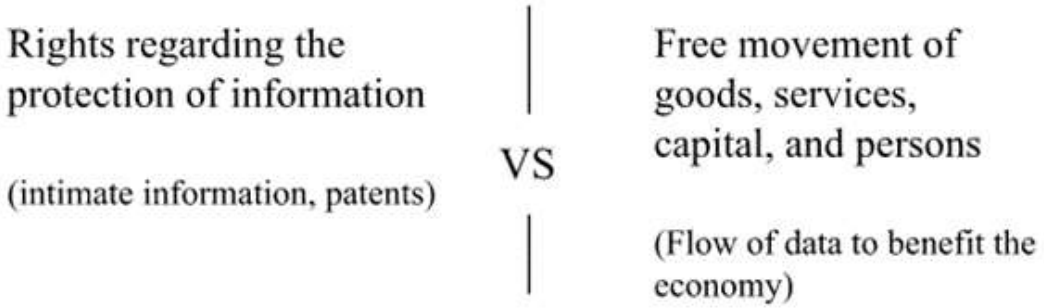


Figure 3 - EU balance between rights and freedoms. Source: prepared by authors

To understand how these often conflicting rights and freedoms are balanced, it is important to highlight that the EU was built on three core principles that provided certainty and efficiency in addressing complex problems.

Conferral	“the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred	Article 5(2), TEU

	upon the Union in the Treaties remain with the Member States"	
Proportionality	"the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties."	Article 5(4), TEU
Subsidiarity	"in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States."	Article 5(3), TEU

Table 3. EU core principles. Source: prepared by authors based on TEU

To deal with data, the EU and the member states have enacted numerous legal documents, the latest being the European strategy for data (European Commission, 2020a). Its purpose is to set a clear path to make the EU a leader in a data-driven society. The strategy sets a vision of a single market for data that allows data to flow freely within the EU, while protecting rights concerning personal data and non personal data (European Commission, 2020a). Specifically for data flows, it opts for an open and assertive approach based on European values (European Commission, 2020a). In other words, it proposes a clear balance between free flow and rights.

Regarding personal data, the member states cooperate with EU institutions to maintain a framework of protection based on the Charter of Fundamental Rights. Taking into consideration the subsidiarity principle, the EU enacted the General Data Protection Regulation (GDPR) to bring homogeneity in the protection of data. Before GDPR, the Directive 95/46/EC only provided guidance on how to regulate the topic internally; as a result each member state enacted laws with different mechanisms of protection and compliance. Additionally, the GDPR has numerous exceptions and special provisions to facilitate international data flows outside the EU without undermining the data protection right.

On non personal data, such as intellectual property, the member states also share regulatory competence with the EU. However, as specified in the next sections, national laws play an important role when setting limits to EU rules. Within the EU, the Data

Governance Act (European Commission, 2020b) and the Regulation on a framework for the free flow of non-personal data (Regulation (EU) 2018/1807) cover mostly how data should be shared across member states and private sectors. A forthcoming Data Act (European Commission, 2022a) will provide rules on the use of data across sectors, including provisions on international data flows outside the EU, and will clarify who can create value from data and under which conditions.

2.2.2. Specific rules for cross-border data flows

As mentioned above, both the GDPR (Art. 45, 46, 49) and the draft for the Data Act (Art. 27) contain provisions to enable international data flows from the EU to third countries. For data flows from third countries to the EU, the overarching rule is that once the data is being processed in the EU, all the internal rules apply, including the commercial agreements of the World Trade organization and other bilateral agreements. Even specific cases of national security and judicial cooperation follow internal rules and exceptions, and tailored treaties.

2.2.2.1. Personal data - GDPR

It is worth mentioning that international "data flow" is interpreted not only as the movement of data from the EU to a third country, but also its processing in a third country (Ustaran, 2019, p. 296). For instance, data package routing falls outside the scope of the GDPR. Additionally, data controllers who must comply with the GDPR are those that are established in the EU, as well as those that offer goods or services or monitor the behavior of people in the EU.

The GDPR mentions the specific case of national and public security stating that they are out of the scope of the regulation. However, these two topics could further strengthen the existing rules or could be used to create specific ones, applied in the context of cross-border data transfers. Therefore, Article 23 of the GDPR provides that member states and the EU can enact specific rules in cases that deal with state security, defense and public security. Moreover, Article 48 mentions transfers requested by a third country judicial institution are usually covered in international agreements such as the mutual legal assistance treaty. This topic is further developed by the Directive (EU) 2016/680.

The GDPR is structured along six principles[3] and sets obligations to data controllers and member states. Additionally, the legal framework is overseen by independent authorities in member states and specific bodies at EU level. The provisions regarding cross-border data flows can be found in Chapter 5. Its application follows a subsidiary logic, meaning that if the first option does not apply to the case, the second option

[3] (1) lawfulness, fairness, and transparency, (2) purpose limitation, (3) data minimisation, (4) accuracy, (5) storage limitation, (6) integrity and confidentiality.

becomes available. Following Casalini et al. (2021)'s outline, the EU has overall opted for a stricter approach setting ex ante conditions for data flows.

As a first option, the controller has to verify if the third country obtained an adequacy decision (Art. 45). Only 14 countries[4] have been granted it so far, while China and the US do not enjoy this status. To be on the adequacy list, the Commission assesses whether the data protection authority is independent, and if the third country participates in regional systems for human rights protection.

Case: Trans-atlantic data transfer US- EU

Between 1998 and 2000, the EU Commision and the U.S. The Department of Commerce developed the Safe Harbor principles, an ad hoc. In 2000, the EU Commission adopted Decision 2000/520/EC stating that those principles granted adequate protection to enable personal data transfers to the US. However, in 2015, the CJEU declared the Safe Harbor (Schrems case I, Maximillian Schrems v Data Protection Commissioner) invalid. Consecutively, there was a EU–US Privacy Shield (Decision (EU) 2016/1250), that the CJEU declared invalid in 2020 (Schrems case II, Maximillian Schrems v Data Protection Commissioner). This decision was made due to concerns regarding US surveillance activities by companies and the government, and inadequate means for EU citizens to enforce their rights guaranteed by the GDPR. Since then, the latest effort has been the initiative of a Trans-Atlantic Data Privacy Framework. In March 2022, the EU and the US agreed in principle, and are working on drafts to transform the initiative into a legal text (European Commision 2022b). The future framework should allow data to flow freely, set rules and safeguards to control the access to data by intelligence agencies in the US, establish a redress system for Europeans, obligations for data processors receiving data from the EU, and monitoring mechanisms.

If the first option is not available, the data controller can transfer personal data if it provides any of the following appropriate safeguards (Art. 46):

Standard data protection clauses approved by the Commission (Art. 93)	The clauses incorporated into contracts contain provisions to provide adequate safeguard to personal data. Its practical application is overseen by the European Commission. In 2021, the Commission published Decision (EU) 2021/9 that set contractual clauses.

[4] These countries are Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay.

An approved certification mechanism (Art. 42)	The data controller in a third country can obtain a certification by an authorized certification body. The certification proves that the data controller complies with the GDPR and lasts 3 years. The certification does not eliminate other obligations set by the GDPR (European Data Protection Board, 2019).
Binding corporate rules (BCRs) (Art. 47)	These are internal corporate privacy rules approved by the Data Protection Authority. These rules allow a company to move data across different jurisdictions, but at the same time creates an compliance obligation.
An approved code of conduct (Art. 40)	It is a document that a data controller in a third country could adopt. The code must contain principles, rights, obligations based on GDPR, and special measures depending on the country's context. Additionally, the data controller should sign enforceable commitments. (European Data Protection Board, 2022)
A legally binding and enforceable instrument between public authorities or bodies	Bilateral/multilateral agreements that ensure data transferred to a third country will be granted similar protection to the EU. Topics of these agreements fall inside the scope of the GDPR, e.g. national security is excluded. (European Data Protection Board, 2020)

Table 4. Appropriate safeguards for transfers

Finally, if the data processor cannot meet any of those safeguards, the last option is to look at the specific exceptions listed in Article 49[5].

2.2.2.2. Non personal data - Data Act Proposal

Overall, the Proposal seeks to allow and incentivize different actors to extract the value of non personal data by creating harmonized rules on fair access and use of data (Art. 1). Therefore, it aims to address concerns regarding the transfer of data to third party

[5] The data controller could only support the data flow with consent (specific, informed and explicit), contracts, substantial public interest, legal claims, vital interest, the personal data is in a public registry, or if the transfer is not repetitive.

countries. Additionally, the proposal clearly states that it does not affect the special rules for international data transfers related to public security, defense and national security (Art. 1.4).

Similar to the GDPR, it proposes a model of setting ex-ante conditions for cross-border data flows but at the same time respects the existence of international agreements. The pertinent provisions on transfer of non personal data outside the EU can be found in Chapter VII, Article 27. The Data Act is still a draft, thus, there is a long process ahead that will lead to the completion of this proposal.

Article 27 integrates a risk approach. The European Commission understands that international non-personal data flows could potentially jeopardize important issues such fundamental rights, provision for remedy, national security, commercially sensitive data, and intellectual property rights (Recital 77). These issues are normally regulated and protected nationally and at the EU level in different legal instruments such as World Trade Organization trade commitments, the General Agreement on Trade in Services and other trade agreements (Explanatory Memorandum). Therefore, the Act calls the providers of data processing services to take reasonable measures to prevent international data flows of non personal data affecting Union law or national law.

Additionally, Article 27 numeral 2 and 3 deal with requests to access non-personal data by judicial or administrative authorities in a third country. According to the proposal, this could only be possible through an international agreement, such as mutual legal assistance treaties. In the absence of it, the proposal mentions a set of possibilities. For instance, the third-country system requires the reasons and proportionality of the transfer request judgment to be specific in character. For the cases where the transfer and access is requested by a third country authority, the data transferred should be the minimum possible, and mandates that the data holder must be notified when feasible.

2.3. United States

Anu Bradford (2021) explains that the US model of digital governance " […] centers on the idea of protecting free speech, free internet and incentives to innovation [and] is part of the broader ideology […] that embraces markets and places less faith in the ability of the government to intervene". For these reasons, the US has strongly advocated for the liberalization of cross-border data flows by labeling its restriction as a trade barrier (USITC, 2013, Chapter 5). Conversely, it recognizes that such free flow involves trade-offs vis-à-vis privacy and national security.

2.3.1. United States' data governance framework

First, free digital trade underpins the US rationale for cross-border data flow. The latter consists of all "commerce conducted by electronic means and includes trade in both goods and services" (Trachtenberg, 2023). The liberalization of international digital

trade supports American arguments in favor of free cross-border data flow (Selby, 2017). Within this rationale, the country's chief motivator is its economic gain in the digital economy. In 2019, it accounted for 9.6% of its GDP (Akhtar & Sutherland, 2021, p.1) and, in 2012, it amounted to a USD 117 billion surplus in digital trade (Selby, 2017). Indeed, under the Trade Promotion Authority (Public Law 114–26, 2015), Congress assigned powers to negotiate trade agreements to the President. One of its key objectives was 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 processing of data".

In recent years, the US has followed a consistent digital trade policy of liberalization. Illustratively, Article 15.8 of the US-South Korea FTA forbids unnecessary barriers to data flows across borders, while recognizing the "importance of protecting personal information" (Chin & Zhao, 2022, p.4). Likewise, both the US-Japan Digital Trade Agreement and the US-Mexico-Canada FTA (USMCA) (i) prohibit restrictions to data flow and data localization; (ii) limit intermediary liability for user-generated content; and (iii) forward consumer protection measures (Trachtenberg, 2023, p.2).

Second, freedom of speech also influences data governance. In the US, the right stems from the First Amendment: "Congress shall make no law (...) abridging the freedom of speech" (US Const., 1791). Accordingly, Biden's 'Declaration on the Future of the Internet' (DFI) (2022) forwards a global Internet of free data flows as necessary to foster societies in which "technology is used to promote pluralism and freedom of expression".

Third, the Supreme Court has repeatedly recognized privacy as a constitutional right that systematically stems from the First, Third, Fourth and Ninth Amendments (Griswold v. Connecticut, 1965; see also: Riley v. California, 2014; Carpenter v. United States, 2018). Its legal framework, nevertheless, is fragmented between Federal- and State-level legislation.

At the Federal-level, protection is segmented. One, the Children's Online Privacy Protection Rule (COPPR, 2013) requires online operators to follow a set of obligations to protect the personal information of children under thirteen years of age. Two, the Health Insurance Portability and Accountability Act (HIPAA) requires health care entities and associated businesses "to protect sensitive patient health information from being disclosed without the patient's consent or knowledge" (CDC, 2022; HHS, 2022a). Three, Section 5 of the Federal Trade Commission Act (FTC Act) assigns the FTC broad powers to prohibit "unfair or deceptive" practices in or affecting commerce, including misleading statements and injuries vis-à-vis data security, consumer, and health privacy (FTC Act, 1914; FTC, n.d.; FTC v. Wyndham Worldwide Corp., 2015).

At the State-level, Connecticut, Colorado, Utah, Virginia and California have enacted comprehensive privacy laws (IAPP, 2023), of which the latter is the most influential.

This is because the California Consumer Privacy Act (CCPA, 2020) applies to any business processing data of California residents, regardless of location, and its regulatory standards have a de facto and de jure effect across State lines (Chander et al., 2021). In short, the CCPA ascribes rights and duties with the aim of "giving consumers control over the personal information businesses collect on them". Correspondingly, US executive policy has consistently recognized that data flow and privacy must be balanced against each other. The Obama Administration forwarded consumer privacy as a core value in the "Digital 2 Dozen" strategy for digital trade (USTR, 2016). Likewise, Biden's DFI (2022) forwards the "[protection of] individuals privacy [while resisting] efforts to splinter the global Internet and [promoting] a free and competitive global economy".

Fourth, national security and law enforcement is a rationale that substantiates both the promotion and restriction of cross-border data flows. On the one hand, flow enables US intelligence activity. Selby (2017) explains that the US holds a comparative advantage in data hosting. This, in turn, contributes to the US government's "comparative advantage for its signals intelligence (SIGINT) agencies in their economies of surveillance of online data compared to [that of] foreign SIGINT agencies" (p.215-216). Indeed, Section 702 of the Foreign Intelligence Surveillance Act (FISA) allows US agencies to conduct "targeted surveillance of foreign persons located outside the [US]" (ODNI, n.d.). Likewise, Executive Order 12333 (EO, 1981) covers "collection by US surveillance authorities of data stored or [that] transited outside of the US geographic borders" (Hoffman, 2021, p.590). Finally, law enforcement also plays a role. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) requires electronic services to "disclose all data in their possession, custody, or control, [...], regardless of the location of the data" when legally warranted to (Daskal, 2018-19, p.11).

On the other hand, flow may be constrained to prevent adversaries from obtaining intelligence about the US. For instance, under the Foreign Investment Risk Review Modernization Act (2018), the Committee on Foreign Investment in the US (CFIUS) may review foreign investments to assess whether they pose a threat to national security. This includes whether transactions may create cybersecurity vulnerabilities or expose citizens personal information. A finding to that end authorizes presidential action to block or mitigate risks (CSIS, 2020). Moreover, the Trump Administration enacted Executive Order 13873 (EO, 2019), thereby prohibiting the acquisition of information and communications technology or services from foreign adversaries, if it posed an undue risk to the acquisition objects themselves, critical infrastructure, the digital economy or the "security and safety of [US] persons." Lastly, the Biden Administration's National Cybersecurity Strategy (White House, 2023) highlights the need for "cross-border regulatory harmonization to prevent cybersecurity requirements from impeding digital trade flows" (p.9).

2.3.2. Specific rules for cross-border data flows

Privacy laws do not expressly refer to cross-border data flows, but impose obligations vis-à-vis data transfers to third parties. Under COPPR and HIPAA, operators must ensure third parties guarantee data confidentiality, security and integrity (Sec. 312.8, COPPR) and enter into contracts that safeguard health privacy and security (HHS, 2019). Under the FTC Act, US firms must comply, even if data flows across borders. For instance, in GMR Transcription Services (FTC, 2014a), the FTC held that a medical and legal transcription company violated the FTC Act by exporting data to transcribers in India, thereby failing to guarantee data security, consumer and health privacy (FTC, 2014b). Under California's CCPA, Section 1798.100(d) requires businesses that share personal information with third parties to enter into a contract that establishes (i) a purpose-limitation for data processing, (ii) an equal level of privacy protection, and (iii) rights to ensure the third party is processing data appropriately and remediate where it is not (Kutner et al, 2022).

National security is the only other policy rationale herein analyzed that may restrict cross-border flows. The US lacks a concrete framework for cross-border transfers that safeguards its national security while simultaneously ascribing legal certainty to data processors. The ongoing debate on TikTok and WeChat illustrates this. The Trump White House (2020) attempted to ban WeChat, a Chinese messaging app, with grounds on national security; but this was limited by freedom of expression. A Court blocked the ban because it "burdened substantially more speech than necessary [to safeguard national security]" (WeChat Users Alliance v. Trump, 2020, p.18). Similarly, in Packingham v. North Carolina (2016, pp.9-10), the Supreme Court found the law cannot completely bar "the exercise of First Amendment rights on websites integral to the fabric of our modern society and culture" (Jaffer, 2023; ACLU, 2023a).

3. Where do these regulations overlap?

The above overview of each data governance framework evinces international trade to be the converging interest of all three polities in promoting cross-border data flow. Nevertheless, this is chiefly accompanied by two caveats: (i) data protection and privacy, and (ii) national security.

Figure 4: convergence and divergence of regulations. Source: prepared by authors.

Suitably, each polity has prescribed instruments aimed at evaluating, instructing and bringing data processors involved in cross-border flows into compliance. Accordingly, this section is fourfold. First, (3.1.) it forwards evidence on the converging interests in international trade. This is followed by convergences and divergences vis-à-vis (3.2.) data protection and privacy, and (3.3.) national security. Finally, (3.4.) it forwards the instruments prescribed by each polity to enable cross-border data flows in the two aforementioned policy fields.

3.1. How does free digital trade influence cross-border data flow?

In short, international free trade of digital goods and services is where the interests of China, the EU, and the US converge, in principle. For example, in the case of China, the RCEP (2020) treaty establishes that each party "shall not prevent cross-border transfer of information by electronic means [for business purposes]" (Art. 12.15(2)). It adds that parties should (i) adopt a legal framework that ensures the "protection of personal information" (Art. 12.8) and (ii) build capability for cybersecurity. Moreover, it forwards that no party shall require data localization as a condition for business to be conducted within its territory (Art. 12.14(2)). However, this may be excepted where a party deems it "necessary to achieve a legitimate public policy objective" or to protect "its essential security interests", and the latter cannot be challenged by other parties (Art. 12.14(3) (a) and (b)).

Additionally, US and EU positions are illustrated by negotiations within the WTO Joint Initiative on Electronic Commerce (2019). The US supports "limiting exceptions to cross-border data flows to 'legitimate public policy objectives'", whereas the EU partially

diverges to explicitly include “a privacy/personal data protection exception” (Ismail, 2023, p.16). In conclusion, trade may be leveraged as a common ground towards governance of cross-border data flows among the three polities. Yet, solving for the caveats requires parties to align their domestic policies over data protection and national security with their trade commitments on cross-border flows and vice-versa.

3.2. How does data protection and privacy influence cross-border data flow?

As hinted, convergence in data protection and privacy is key for cross-border data flows because polities expect one another to maintain equal levels of protection once their citizens’ data flow overseas. As seen below, the latter partially overlaps among all three polities.

DATA PROTECTION AND PRIVACY	EU	US-CA[1]	PRC
	GDPR (2016)	CCPA (2018)	PIPL (2021), DSL (2021)
Notification in data collection	Arts. 13(f); 14(f), GDPR	1798.100(a)(c), CCPA	Art. 17, PIPL
Consent mechanism	Arts. 6, 7, 49, GDPR	NA	Art. 13, PIPL
Purpose specification	Art. 5(b), GDPR	1798.100(a)(1)(2), (c), CCPA	Art. 6, PIPL
Collection limitation / proportionality	Art. 5(c), GDPR	1798.100(a)(1)(2), (c), CCPA	Arts. 5, 6, PIPL
Data retention limitation	Art.5(e), GDPR	1798.100(a)(3),(c), CCPA	Art. 19, PIPL

Security and confidentiality	Arts. 5(f), 32 GDPR	1798.100(e), CCPA	Art. 10, PIPL
Data accuracy	Arts. 5(d), 32, GDPR	NA	Art. 46, PIPL
Sensitive data additional measures	Art. 9, GDPR	1798.121, CCPA 1798.100(a)(2), CCPA	Art. 21, DSL
Independent oversight in organization (i.e., DPO)	Arts. 37, 38, 39, GDPR	NA	Art. 58, PIPL
Breach notification	Arts. 33, 34, GDPR	1798.82(a), Civil Code	Art. 57, PIPL
Right to review of automated decision	Arts. 22, GDPR	NA	Art. 24, PIPL
User rights (i.e., access, objection, deletion, rectification, data portability)	Arts. 15, 16, 17, 20, 21, GDPR	1798.105, CCPA	Art. 43, CSL Art. 15, PIPL
Ombudsman (Public Authority)	Chapter VI, GDPR	1798.199.10, CCPA	Art. 11, PIPL

Table 5: Legal basis in the US, EU and PRC. Source: authors' own production (adapted from Casalini et al., 2021).

[1] The framework compares privacy and data protection rules in the PRC, EU and US. For the latter, it focuses exclusively on the Californian legal framework as it is the only one that sets forth substantive

rules with enough legal certainty for comparison. Notably, the FTC Act coupled with FTC's enforcement actions may legitimize the existence of some of the cross-compared provisions above at the federal level. But, these lack both **(i)** legal certainty and **(ii)** effects towards all (*erga omnes*) because **(i)** the FTC Act is too vague and **(ii)** the enforcement actions are binding only to the parties of a case.

3.3. How does national security influence cross-border data flow?

Notably, commonalities here do not support convergence on the basis of substance due to the adversarial character of national security concerns. That is, each polity may agree as to their national security policy, nevertheless, these are pursued against each other and do not constitute a common normative ground to further cross-border data flows. However, the existence of national security concerns may support convergence in procedure for international transfers of data.

In the EU and the US, there are currently no procedural rules for cross-border data transfers that ascribe this level of legal certainty on the grounds of national security. Indeed, the former lacks full competence over national security issues (TFEU, Art. 72, & TEU, Art. 4(2)). The latter illustrates, for instance through the TikTok case, that there is increasing attention to the risk data may pose to national security, but lacks a clear legal basis. China, on the other hand, is implementing its "数据分类分级保护制度" (categorized and graded protection system for data) (DSL, Art. 21). In this classification, "categorized" refers to data type and "graded" to the level of sensitivity for national security, the economy, people's livelihoods or major public interests.

Thus, China has legal means to restrict cross-border data flows both on personal information protection and national security grounds. It should be in the interest of all polities to prescribe instruments that ensure that their national security is not compromised while simultaneously granting legal certainty to actors involved in cross-border data flows, as it occurs in the field of data protection.

3.4. Compliance and conformity assessment instruments for cross-border data flows

Every legal framework has different ways to enable cross-border data flows. However, while the US is mostly restricted to SCCs, the EU's GDPR and China's PIPL allow for other instruments such as Certification Mechanisms and Binding Corporate Rules. The EU is the only actor that uses the comparative instrument of an Adequacy Decision and China, as seen in chapter 3.3, uniquely applies an assessment instrument to measure risk regarding national security.

Instruments enabling data flows	GDPR (2016)	CCPA (2018)	PIPL (2021), DSL (2021)
Adequacy Decision	Art 45 GDPR	NA	Na
Standard Contractual Clauses (SCC)	Art 46. 2 c) d) , Art 46. 3 a), Art 93.2 GDPR	Sec. 1789.100(d)	Art. 38 (3), PIPL
Certification Mechanism	Art 46. 2 f), Art 42, Art 43 GDPR	NA	Art. 38 (2), PIPL
Binding Corporate Rules	Art 46.2 b), Art 47 GDPR	NA	NA
Code of Conduct	Art 46. 2 e), Art 40, Art 42 GDPR	NA	NA
Security Assessment Measures[1]	NA	NA	Art. 31, DSL; Art. 40, PIPL

Table 6: Instruments to enable cross-border flows (inc. the privacy, national security, trade rationale)

[1] Only instrument that also covers national security concerns.

Notably, there are two dimensions to these processes vis-à-vis restriction or promotion of cross-border data flow. First, their regulatory and economic stringency on the data processors. That is, the more stringent, the more expensive it is to comply, the more restrictive to cross-border flow. For example, an adequacy decision or BCRs are more stringent than SCCs . Second, the level of relative harmonization of the processes used by each polity to enable cross-border data flow. This is, if polities use the same regulatory processes, processors can simultaneously and, thus, more efficiently comply with more than one country's legal framework. Consequently, a given process may be quite stringent under the first dimension, but if it is harmonized with processes adopted by other polities, the efficiencies derived from the second dimension may compensate for the inefficiencies from the first.

On this note, data localization is a measure that allows for digital markets access, as all the above processes; yet, unlike them, it does not promote cross-border data flow. Data localization as such is only mandated in China when the data handler processes important data and personal information (CSL, Art. 37; PIPL, Art. 40). This idea, although restrictive, is explorable as an experimental solution to the dilemma between cross-border data transfers and national security, as it grants a form of legal certainty. Yet, as unilateral means to hinder data flows, this instrument is contested (Chander, 2020).

4. Policy Recommendations

This section proposes concrete recommendations to the G20 Digital Economy Ministers, specifically the authorities of China, US, and EU, to facilitate cross-border data flows. These are divided into (4.1.) stabilizing; thus, amendments or extensions of existing practices, and (4.2.) transformative measures.

4.1. Stabilizing measures: improving existing practices

4.1.1. Build a repository of existing governance frameworks

The first step to foster data transfers is the understanding of the existing legal frameworks and the identification of reasons that may hinder free flows of data. It is, thus, recommended that international organizations leverage this report to create a repository of existing governance frameworks. They should incorporate in this repository an in-depth study of the aforementioned principles and values for each polity, and continue to explore areas of potential convergence.

4.1.2. Enhance technical and data-based interoperability: data standards, granularity, API

Interoperability can be thought of in four layers (Palfrey and Gasser 2012, pp.6-7). The first is technical, and refers to the connection of systems and the exchange of signals through an interface. The second concerns data. Here, interoperability is achieved when interacting actors can read, process and handle transmitted information. These first layers can be achieved through the development of data standards that define, structure and clarify use and management of data. In addition, granularity and a data classification can help firms to comply with different regulations. Moreover, Application Programming Interfaces (APIs) can provide authentication and secure data exchanges.

4.1.3. Strengthen human-based interoperability: FTAs and multilateral framework

The third layer of interoperability is a human layer, thus, “whether [the actors] are willing to put effort into working together” like creating a common language (p.7). As seen in the previous section, the policy domains in which there are higher points of

convergence should be leveraged. The starting point to achieve this could be based on trade agreements, in which the three polities have existing commonalities and in which economic interests may converge. Bilateral and multilateral trade agreements could incorporate provisions that include duties to standardize data protection frameworks domestically, and make processing of data more transparent. Other considerations could include encryption keys to boost confidence between parties.

To tackle the fourth layer of interoperability, a multi stakeholder, multilateral and multidisciplinary governance framework should be institutionalized to unlock the value of cross-border data flows while safeguarding the interests of each polity and enhancing legal certainty.

4.1.4. Leverage standard contractual clauses

It is also suggested that countries continue to harmonize and rely on standard contractual clauses to facilitate data transfers. SCCs can be used by private parties in their contractual agreements and have the advantages of being predictable, pre-approved, standardized and easy to implement. Importantly, they assign legal liability to cross-border data processors, regardless of their location, by replicating domestic law into contractual terms. Consequently, the latter becomes enforceable against these data processors through their own polity's judicial system on the basis of contractual liability. As seen in Table 6, the three polities currently use SCCs and this instrument could, thus, be further adopted.

4.2. Transformative measures: exploring new ways how data flows across borders

4.2.1. Consider privacy-enhancing technologies

Other approaches that have not yet been fully explored include the adoption of Privacy-Enhancing Technologies (PETs). This is “a collection of digital technologies, approaches and tools that permit data processing and analysis while protecting the confidentiality, and in some cases also the integrity and availability, of the data and, thus, the privacy of the data subjects and commercial interests of data controllers” (OECD, 2023, p.13). Some techniques that could be experimented are differential privacy, pseudo anonymization, homomorphic encryption or federated analysis, among others[6].

[6] **Differential privacy techniques** “make small changes (add noise) to the raw data to mask the details of individual inputs, while maintaining the explanatory power of the data.” **Pseudo anonymization** is a form of de-identification (OECD, 2023, p.16-17) **Homomorphic encryption** implies that “data is encrypted before sharing so that it can be analyzed, but not decoded into the original information.” **Federated analysis** means that parties share the “insights from the analysis of their data without sharing the data itself.” (WEF, 2023, p.8).

4.2.2. Establish legally-adequate data hubs in FTZs located in trusted third-parties

In addition to technical tools, experimental mechanisms may be examined. Escrow agreements may serve as inspiration. These are contractual arrangements by which parties designate a third party ("escrow agent") that guarantees accountability, overseeing, monitoring and compliance to a transaction. The agent "holds in escrow certain assets, documents, and/or money deposited by such parties until a contractual condition is fulfilled" (Cornell Law School, 2021). This rationale may be coupled with the concept of free-trade zones (FTZ) for the free flow of data. For instance, the aforementioned international data hub in China's Hainan FTZ takes heed of technical, business, security and regulatory cross-cutting conditions to become a safe-haven for cross-border data transfer from and into China (Plattform Industrie 4.0, 2020).

The polities may engage in multilateral negotiations with each other and third party countries (escrows) to assign a FTZ for cross-border data flows within their territories. This would include agreed upon institutional and technical frameworks on security and data protection that satisfy each polity vis-à-vis their domestic law and geopolitical concerns. Accordingly, these FTZs would automatically be deemed adequate by each polity on the basis of both data protection and national security. The technical and institutional aspects would be managed by the escrow, but fully overseen and disputable by the polities. Lastly, negotiations could be incrementally pursued, starting from data flows within industries that are least sensitive to data protection and national security up to more sensitive ones. As such, each negotiation milestone may be leveraged to achieve success in the next.

Many arguments favor this arrangement. First, it works as a system of checks and balances by design (Lessig, 1999, 2006) because each polity is incentivized to inform on technical vulnerabilities. Otherwise, they risk having others exploit these unreported loopholes. Second, it ascribes legal certainty for cross-border data processors to engage in digital trade and have access to the three wealthiest markets in the world. Third, rather than requiring data localization, it economically incentivizes an adapted version of it; that enjoys its security, while enabling cross-border flows. Fourth, even though this process may be more stringent than others and, thus, inefficient vis-à-vis promotion of data flow, harmonization among all three polities may compensate for it.

4.2.3. Enact a court with transnational jurisdiction within judiciary branch

As explained in section 3.2 (p. 21), China and the US face barriers to transfer data from the EU in view of the latter's legal framework, particularly GDPR and CJEU's Schrems I and II. Although the ongoing US-EU "agreement in principle" over trans-atlantic data transfer includes a "Data Protection Review Court" (WH, 2022; EC, 2022c), important stakeholders have argued that this does not provide an adequate level of protection

because, among others, it lacks sufficient independence from the executive branch (NOYB, 2023; Bertuzzi, 2023; EDPB, 2023, paras. 216, 222-228).

The polities, therefore, could explore enacting courts with transnational jurisdiction within their judiciaries. As explained by Jessup (1956), transnational law refers to “all law which regulates actions or events that transcend national frontiers”. Indeed, the jurisdiction of courts and laws have long transcended national boundaries in specific areas, such as family law (Romano, 2020) and American antitrust law (Kraus, 2014). This proposal differs in that it forwards the institution of courts domestically to safeguard rights ascribed by foreign law to persons situated abroad. The legitimacy to bring a case before such a court would stem from the terms of GDPR's jurisdictional scope (Article 3). That is, for processors not established in the EU, if they (1) offer goods or services or (2) monitor the behavior of persons situated within EU territory.

This keeps decision-making on data protection and national security trade-offs completely within one polity's (i.e., US) own domestic enforcement and adjudicative jurisdiction, while enabling the internal enforcement of a law enacted by the prescriptive jurisdiction of a foreign actor (i.e., EU). Even though this will affect national security, the latter has been fairly safeguarded while being balanced against other rights before. For instance, the US Supreme Court has never "upheld an injunction against speech on national security grounds" (ACLU, 2023b); and yet, the nation remains secure. One limitation for China is that its "judiciary is regularly criticized for the lack of (meaningful) independence," specially in the West (Peerenboom, 2012, p.69). Thus, even this proposal would probably fail to satisfy EU standards for cross border data flows.

Lastly, this experiment would have larger policy implications for digital governance. This is because the cross border character of the latter has disrupted all legal concepts historically developed in association with a physical territory, such as jurisdiction and sovereignty. If successful, this could be the birth of a transnational judiciary and inform dispute resolution in other areas of digital policy that are increasingly contentious across borders, such as remote employment.

4.3. Special considerations

There are other fields of a larger policy debate that also affect cross-border data flows that are not encompassed by the above recommendations, such as the (1) the gathering and production of electronic evidence overseas for judicial purposes and (2) different standards of freedom expression across countries, specially in relation to content moderation.

5. Conclusion

In conclusion, allowing for cross-border data flows for trade and growth in the digital economy, but without compromising on privacy/data protection and national security, is a priority for the PRC, the EU and the US alike. To find convergence between these polities, this brief compares their values and principles as well as regulatory frameworks and transfer-enabling instruments. However, for certain regulations, e.g. the DSL and PIPL, there is almost no precedent in how the rules and guidelines are implemented and the EU's Data Act is still in proposal stage.

Nonetheless, through the comparison, this brief identifies convergence in international free trade of digital goods and services; and divergence in data protection between US and EU, and in national security from these two vis-à-vis China. Furthermore, the instruments indicate overlaps, which could be further fostered to allow for cross-border data flows. Here, potential barriers stemming from an increase in stringency for data processors should be mitigated through harmonization of procedures.

Overall, the G20 Digital Economy Ministers should implement the stabilizing and explore the possibility of the transformative measures to improve convergence in the regulation of cross-border data flows for the sake of a thriving digital economy while safeguarding their nation's security and privacy rationales.

References

Akhtar S. & Sutherland, M. (2021). Digital Trade and U.S. Trade Policy. Congressional Research Service. Retrieved March 20 fromhttps://crsreports.congress.gov/product/pdf/R/R44565

American Civil Liberties Union. (ACLU). (2023a). ACLU Condemns House Foreign Affairs Committee Vote on TikTok Ban Bill. Retrieved March 20, 2023 from https://www.aclu.org/press-releases/aclu-condemns-house-foreign-affairs-committee-vote-on-tiktok-ban-bill

American Civil Liberties Union. (ACLU). (2023b). Freedom of Expression. Retrieved April 18, 2023 from https://www.aclu.org/other/freedom-expression

Arcesati, R. (2023, February 23). Fragmenting data governance – Europe needs a strategy to live with China. Merics. Retrieved March 28, 2023 from https://merics.org/en/short-analysis/fragmenting-data-governance-europe-needs-strategy-live-china

Bertuzzi L. (2023) MEPs to call for renegotiation of EU-US data transfer framework. EURACTIV. Retrieved April 18, 2023 from https://www.euractiv.com/section/data-privacy/news/meps-to-call-for-renegotiation-of-eu-us-data-transfer-framework/

Biden's White House. (2022). Declaration for the Future of the Internet. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

Bradford, A. (2020, June 17). How Europe Rules the Digital Economy. Project Syndicate. Retrieved March 28, 2023 from https://www.project-syndicate.org/magazine/brussels-effect-digital-economy-by-anu-bradford-2020-04

Bradford, A. [Tilburg University]. (2021). The Future of Liberal Democracy in the Era of Surveillance Capitalism and Digital Authoritarianism [Video]. Keynote lecture delivered in the Competition and Market Regulation LL.M. Track. https://www.youtube.com/watch?v=p_xyagWJy3U

Brishan, M., Devesa, T., Samandari, H., Smit, S., Seong, J., White, O., & Woetzel, J. (2022, November 15). Global flows: The ties that bind in an interconnected world. Discussion Paper. McKinsey Global Institute. Retrieved March 19, 2023 from https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world#/

California Consumer Privacy Act (CCPA). (2020 & rev. 2023). State of California, Department of Justice, Attorney's General Office. https://oag.ca.gov/privacy/ccpa

Casalini, F., González, J. C., & Nemoto, T. (2021). Mapping commonalities in regulatory approaches to cross-border data transfers. OECD Trade Policy Working Papers, n°248 https://doi.org/10.1787/ca9f974e-en

Carpenter v. United States. (2017). Oyez. Retrieved April 1, 2023, from https://www.oyez.org/cases/2017/16-402

Center for Disease Control and Prevention (CDC). (2022). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Retrieved April 6, 2023 from https://www.cdc.gov/phlp/publications/topic/hipaa.html#security-rule

Center for Strategic & International Studies. (CSIS). (2020). TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications. Retrieved March 23, 2023 from https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications

Chan, S. (2018). Cybersecurity under Xi Jinping. Center for the digital future. https://www.digitalcenter.org/wp-content/uploads/2018/01/Cybersecurity-under-Xi-Jinping-analysis.pdf

Chander, A. (2020). Is Data Localization a Solution for Schrems II? In: Journal of Economic Law 23(3). https://doi.org/10.1093/jiel/jgaa024

Chander, A., Kaminski, M. & McGeveran, W. (2021). Catalyzing Privacy Law. Minnesota Law Review. 3305. Retrieved April 1, 2023 from https://scholarship.law.umn.edu/mlr/3305

Charter of Fundamental Rights of the European Union. (2012). Official Journal of the European Union. 2012/C 326/02. http://data.europa.eu/eli/treaty/char_2012/oj

Children's Online Privacy Protection Rule. 78 FR 4008. (2013). https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Chin, Y., & Zhao, J. (2022), Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. Laws 11(63). Retrieved March 29, 2023 from https://doi.org/10.3390/laws11040063

China Macro Group. (2022). China clarifies its data security regulation to govern cross-border data flows. Retrieved March 19, 2023 from https://www.chinamacro.ch/post/china-clarifies-its-data-security-regulation-to-govern-cross-border-data-flows

Cornell Law School. (2021). Escrow agreement. Retrieved April 18, 2023 from https://www.law.cornell.edu/wex/escrow_agreement#:~:text=The%20escrow%20agreement%20is%20a,a%20contractual%20condition%20is%20fulfilled.

Creemers, R. (2022). China's emerging data protection framework. In: Journal of Cybersecurity, Volume 8, Issue 1, 2022. Retrieved March 29, 2023 from: https://academic.oup.com/cybersecurity/Article/8/1/tyac011/6674794

Cybersecurity & Infrastructure Security Agency (CISA). (2021, February 1). What is Cybersecurity? Retrieved April 2, 2023 from https://www.cisa.gov/news-events/news/what-cybersecurity#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information

Cyberspace Administration of China (CAC). (2022, June 9). Shùjù chūjìng ānquán pínggū bànfǎ 数据出境安全评估办法 [Outbound Data Transfer Security Assessment Measures]. Retrieved March 23, 2023 from http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review.

Criddle, C., McMorrow, R., & Murphy, H. (2023, March 22). TikTok caught in US-China battle over its powerful algorithm. Financial Times. Retrieved March 26, 2023 from https://www.ft.com/content/b9f3b5a8-19ae-407f-be4b-e2536617b0f8

Daskal J. (2019). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Retrieved March 23, 2023 from: https://heinonline.org/HOL/P?h=hein.journals/slro71&i=9

Decision 2000/520/EC. On the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce. http://data.europa.eu/eli/dec/2000/520/oj

Decision (EU) 2016/1250. On the adequacy of the protection provided by the EU-U.S. Privacy Shield. http://data.europa.eu/eli/dec_impl/2016/1250/oj

Decision (EU) 2021/9. 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. http://data.europa.eu/eli/dec_impl/2021/914/oj

DigiChina. (2018, June 29). Translation: Cybersecurity Law of the People's Republic of China Retrieved March 23, 2023 from https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

DigiChina. (2021, June 29). Translation: Data Security Law of the People's Republic of China. Retrieved March 23, 2023 from https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

DigiChina. (2021, September 7). Translation: Personal Information Protection Law of the People's Republic of China. Retrieved March 23, 2023 from https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

DigiChina. (2022, July 8). Translation: Outbound Data Transfer Security Assessment Measures. Retrieved March 23, 2023 from https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/

Directive 95/46/EC. On the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://data.europa.eu/eli/dir/1995/46/oj

Directive (EU) 2016/680. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data. http://data.europa.eu/eli/dir/2016/680/oj

Desai, A. (2023). US State Comprehensive Privacy Laws Report – Overview. International Association of Privacy Professionals. Retrieved March 29, 2023 from https://iapp.org/resources/Article/us-state-privacy-laws-overview/

European Commission.(2020a). A European Strategy for data. COM/2020/66 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN

European Commission. (2020b). Proposal for a Regulation of the European Parliament and of the Council on European data data governance (Data Governance Act). COM/2020/767 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767

European Commission. (2022a). Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). COM/2022/68 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0068

European Commission. (2022b). European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. Retrieved April 1, 2023 from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

European Commission. (EC). (2022c). European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

European Commission. (n.d). EU position in world trade. Retrieved March 23, 2023 from https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/eu-position-world-trade_en

European Data Protection Board. (2019). Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679). Version 3.0. Retrieved March 23, 2023 from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

European Data Protection Board. (2020). Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies. Version 2.0. Retrieved March 23, 2023 from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf

European Data Protection Board. (2022). Guidelines 04/2021 on Codes of Conduct as tools for Transfers Version 2.0. Retrieved March 23, 2023 from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf

European Data Protection Board. (EDPB). (2023). Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. Retrieved April 18, 2023 from https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf

European Data Protection Supervisor. (EDPS). (2019). Government access to data in third countries: Final Report. Retrieved March 23, 2023 fromhttps://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

Executive Order. (EO, 1981). 12333. United States intelligence activities. 6 FR 59941, 3 CFR

Executive Order. (EO) (2019). 13873. Securing the Information and Communications Technology and Services Supply Chain. 84 FR 22689.

Federal Data Protection Act (Bundesdatenschutzgesetz — BDSG). (1978). NCJ 53219.

Federal Trade Commission Act. (1914). 15 USC Chapter 2, Subchapter I. http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim

Federal Trade Commission. (FTC). (n.d.). Privacy and Security Enforcement. Retrieved March 21, 2023 from https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacysecurity-enforcement

Federal Trade Commission. (FTC). (2014a). In the Matter of GMR Transcription Service, Inc. - Decision and Order.Retrieved March 28, 2023 fromhttps://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf

Federal Trade Commission. (FTC). (2014b). FTC Approves Final Order in Case Against GMR Transcription Services. Retrieved March 28, 2023 fromhttps://www.ftc.gov/news-events/news/press-releases/2014/08/ftc-approves-final-order-case-against-gmr-transcription-services

Federal Trade Commission (FTC) v. Wyndham Worldwide Corp., (2015). United States Court of Appeal for the Third Circuit. No. 14-3514. https://www.ftc.gov/system/files/documents/cases/150824wyndhamopinion.pdf

Fefer, R. (2020, March 26). Data Flows, Online Privacy, and Trade Policy. Congressional Research Service.

Ferracane, M. F., Lee-Makiyama, H., & Van Der Marel, E. (2018). Digital Trade Restrictiveness Index. European Center for International Political Economy (ECIPE). Retrieved March 20, 2023 from https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

Foreign Intelligence Surveillance Act. (FISA). 92 Stat. 1783.

Foreign Investment Risk Review Modernization Act. (2018). H. R. 5515—538. Retrieved April 2, 2023, from https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf

G20 Indonesia. (2022). G20 Bali Leaders' Declaration.

Griswold v. Connecticut. (1965). Oyez. Retrieved April 1, 2023, from https://www.oyez.org/cases/1964/496

Health Insurance Portability and Accountability Act. (HIPAA). Pub. L. No. 104-191, § 264, 110 Stat.1936.

Health and Human Services. (HHS). (2019). Business Associates. Retrieved March 23, 2023 from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

Health and Human Services. (HHS). (2022a). The HIPAA Privacy Rule. Retrieved March 23, 2023 from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule&text=The%20Rule%20requires%20appropriate%20safeguards,information%20without%20an%20individual's%20authorization

Hoffman, D. A. (2021). Schrems II and tiktok: two sides of the same coin. North Carolina Journal of Law & Technology, 22(4), 573-616. Retrieved April 2, 2023 from https://heinonline.org/HOL/P?h=hein.journals/ncjl22&i=605

Horsley, J. (2021, January 26). How will China's privacy law apply to the Chinese state? New America. Retrieved April 2, 2023 from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/

IAPP. (2023). US State Comprehensive Privacy Laws - Overview. Retrieved March 26, 2023 from https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_overview.pdf

Ismail, Y. (2023). The Evolving Context and Dynamics of the WTO Joint Initiative on E-commerce: The fifth-year stocktake and prospects for 2023. Geneva, Switzerland. International Institute for Sustainable Development and CUTS International. Retrieved April 1, 2023 from: https://www.iisd.org/system/files/2023-04/wto-joint-initiative-e-commerce-fifth-year-stocktake-en.pdf

ISO/IEC 20889:2018. Privacy enhancing data de-identification terminology and classification of techniques. Retrieved March 29, 2023 from https://www.iso.org/standard/69373.html

Jaffer, J. (2023). There's a Problem With Banning TikTok. It's Called the First Amendment. The New York Times.Retrieved April 2, 2023 fromhttps://www.nytimes.com/2023/03/24/opinion/tiktok-ban-first-amendment.html

Jessup P. C. (1956) Transnational Law II. Storrs lecture series delivered at Yale University.

Kraus E. F. (2014). Extraterritoriality & Antitrust: A Perspective on the U.S. Experience. Federal Trade Commission. Retrieved April 18, 2023 from https://www.ftc.gov/system/files/attachments/key-speeches-presentations/extraterritoriality.pdf

Kutner et al. (2022). Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA. Cooley. Retrieved March 21, 2023 from https://cdp.cooley.com/cross-border-data-transfers-pipl-vs-gdpr-vs-ccpa/#_ftn5

Ladley, J. (2012). Data Governance How to Design, Deploy, and Sustain an Effective Data Governance Program. 1st edition. Waltham, Mass: Morgan Kaufmann.

Le Monde. (2023, March 24). France bans TikTok from public employee work phones. Retrieved March 28, 2023 from https://www.lemonde.fr/en/politics/article/2023/03/24/france-bans-tiktok-from-public-employee-work-phones_6020523_5.html

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. Harvard Law Review, 113(2), pp. 501-549. Retrieved April 18, 2023 from https://doi.org/10.2307/1342331

Lessig, L. (2006). Code: And Other Laws of Cyberspace, Version 2.0. Tiger Prints. Retrieved April 16, 2023 from https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1183&context=cheer

Maximillian Schrems v Data Protection Commissioner. (2015).ECLI:EU:C:2015:650. Judgment of the Court (Grand Chamber). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362

Maximillian Schrems v Data Protection Commissioner. (2020). ECLI:EU:C:2020:559. Judgment of the Court (Grand Chamber). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311

Ministry of Commerce People's Republic of China (MOFCOM). (2018). China and Singapore Conclude Negotiations on Upgrading Free Trade Agreement. Retrieved March 21, 2023 from http://fta.mofcom.gov.cn/enarticle/ensingapore/ensingaporenews/201811/39321_1.html

National People's Congress (NPC). (2016, November 11). Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China]. Retrieved March 23, 2023 from http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

National People's Congress (NPC). (2018, June 12). 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]. Retrieved March 23, 2023 from

http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml

National People's Congress (NPC). (2021a, October 6). 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]. Retrieved March 23, 2023 from http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

National People's Congress (NPC). (2021b, August 20). 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]. Retrieved March 23, 2023 from http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

None of Your Business. (NOYB). (2022). Six months of "agreement in principle", EU-USE agreement in fact still missing. Retrieved April 18, 2023 from https://noyb.eu/en/6-months-agreement-principle-eu-us-agreement-fact-still-missing

Palfrey, J. & Gasser, U. (2012). Interop: The Promise and Perils of Highly Interconnected Systems. The Berkman Klein Center for Internet & Society at Harvard University.

Peerenboom R. (2012). Judicial Independence in China: Lessons for Global Rule of Law Promotion. Cambridge University Press. Retrieved April 18, 2023 from https://doi-org.acces-distant.sciencespo.fr/10.1017/CBO9780511809484

People's Daily. (2022, September 6). Xíjìnpíng: Méiyǒu wǎngluò ānquán jiù méiyǒu guójiā ānquán习近平：没有网络安全就没有国家安全 [Xi Jinping: There is no national security without cybersecurity]. Retrieved March 23, 2023 from http://politics.people.com.cn/n1/2022/0906/c1001-32520806.html

People's Daily. (2023, March 11). Guówùyuàn jīgòu gǎigé fāng'àn 国务院机构改革方案 [State Council Institutional Reform Program]. Retrieved March 23, 2023 from http://lianghui.people.com.cn/2023/n1/2023/0311/c452482-32641702.html

Platform Industrie 4.0. (2020). Cross-Border Data Transfer Piloting – Hainan Free Trade Port. Retrieved April 21, 2023 from https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/China/Policy-Briefing-Cross-BorderDataTransfer.pdf?__blob=publicationFile&v=2

Public Law 114–26. (2015). Defending Public Safety Employees' Retirement Act. https://www.congress.gov/114/plaws/publ26/PLAW-114publ26.pdf

Romano G. P. (2020) Hacia la creación de tribunales transnacionales para las familias transnacionales: el ejemplo de la responsabilidad parental. La Ley: Mediación y Arbitraje, Iss. 3. Retrieved April 18, 2023 from https://archive-ouverte.unige.ch/unige:143199

The Economist. (2017, May 11). The world's most valuable resource is no longer oil, but data. Retrieved March 28, 2023 from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The Clarifying Lawful Overseas Use of Data Act. (CLOUD Act). S.2383 — 115th Congress (2017-2018).

The People's Government of Hainan Province (Hainan Government). (2023, March 7). Zhīchí hǎinán tànsuǒ guójì shùjù zhōngxīn shìdiǎn 支持海南探索国际数据中心试点 [Hainan to explore the possibility of an international data hub]. Retrieved April 3, 2023 from https://www.hainan.gov.cn/hainan/szfldhd/202303/d55d9f928ee045a2ad7ba13dfae21114.shtml

Trachtenberg, D.(2023). Digital Trade and Data Policy: Select Key Issues. Congressional Research Service. Retrieved March 20, 2023 fromhttps://crsreports.congress.gov/product/pdf/IF/IF12347

Treaty on European Union. (2007). Official Journal of the European Communities. C326/13. http://data.europa.eu/eli/treaty/teu_2012/oj

Trump White House. (2020). Executive Order on Addressing the Threat Posed by WeChat. Retrieved March 28, 2023 from https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/

Torreblanca, J. I. (2021). Technology. In: European Council on Foreign Relations, Stiftung Mercator, The Power Atlas (pp. 38-61). Retrieved March 28, 2023 from https://ecfr.eu/wp-content/uploads/power-atlas.pdf

OECD. (2014). OECD Recommendation on Digital Government Strategies. Retrieved March 28, 2023 from https://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm

OECD. (2017). OECD Digital Economy Outlook 2017. Retrieved March 28, 2023 from https://doi.org/10.1787/9789264276284-en

OECD. (2019). The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/059814a7-en

OECD. (2020). Mapping Approaches to data and data flows. Report for the G20 Digital Economy Task Force. Retrieved April 6, 2023 from https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf

OECD. (2023). Emerging privacy-enhancing technologies. Current regulatory and policy approaches.OECD Digital Economy Papers, No. 351. https://doi.org/10.1787/20716826

Office of the Director of National Intelligence. (ODNI). (n.d.). Section 702 - Overview. https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf

Office of the United States Trade Representative (USTR). (2016). The Digital 2 Dozen.Retrieved March 27, 2023 from https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf

Packingham v. North Carolina. (2016). Supreme Court of the United States. Retrieved March 27, 2023 from https://www.supremecourt.gov/opinions/16pdf/15-1194_08l1.pdf

Regional Comprehensive Economic Partnership Agreement (RCEP). (2020). Chapter 12, Electronic commerce. Retrieved March 29, 2023 from https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf

Regulation (EU) 2016/679. 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). http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2018/1807. On a framework for the free flow of non-personal data in the European Union. http://data.europa.eu/eli/reg/2018/1807/oj

Regulation (EU) 2019/881. On information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). http://data.europa.eu/eli/reg/2019/881/oj

Riley v. California. (2014). Oyez. Retrieved April 1, 2023, from https://www.oyez.org/cases/2013/13-132

Schmitt M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. Retrieved April 18, 2023 from https://doi-org.acces-distant.sciencespo.fr/10.1017/9781316822524

Selby, J. (2017). Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?. International Journal of Law and Information Technology, 25(3), 213–232. https://doi.org/10.1093/ijlit/eax010

Şimşek, C. (2021, August 21). [Interview] International trends in data protection and privacy regulations: 3 questions to Fabian Delcros.Sciences Po. Chair Digital, Governance, and Sovereignty. Retrieved April 2, 2023 from https://www.sciencespo.fr/public/chaire-numerique/en/2021/08/26/international-trends-in-data-protection-and-privacy-regulations-3-questions-to-fabian-delcros/

United States International Trade Commission (USITC). (2013). Digital Trade in the U.S. and Global Economies, Part 1. Retrieved April 3, 2023 from: https://www.usitc.gov/publications/332/pub4415.pdf

U.S. Const. (1791). amend. I

Ustaran, E. (2018). European Data Protection Law and Practice. Second Edition. International Association of Privacy Professionals.

WeChat Users Alliance v. Trump. (2020). United States District Court Northern District of California. San Francisco Division. Case No. 20-cv-05910-LB. Retrieved April 9, 2023 from https://www.courtlistener.com/docket/17470217/59/us-wechat-users-alliance-v-trump/

White House. (WH). (2022). Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework. Retrieved April 18, 2023 from https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

White House. (2023). National Cybersecurity Strategy. Retrieved April 9, 2023 from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

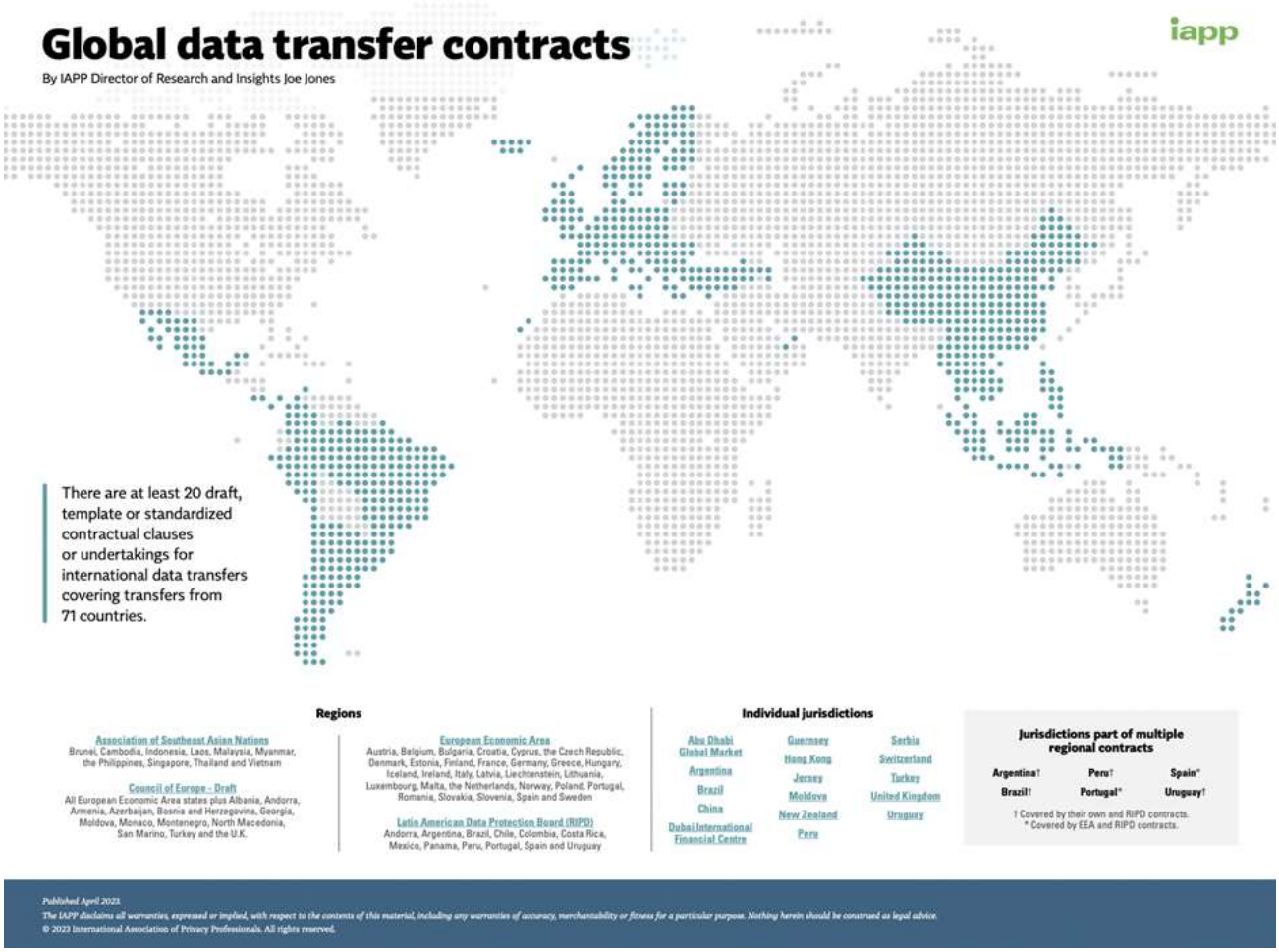
World Economic Forum (WEF). (2023, January 17). We must protect cross-border data flows — here's why. Retrieved April 3, 2023 from https://www.weforum.org/agenda/2023/01/data-flows-cross-border-wef23/

World Trade Organization. (WTO). (2019). Joint Statement on Electronic Commerce. WT/L/1056.

Xinhua News Agency (Xinhua). (2021, July 4). Guójiā wǎng xìn bàn: Guānyú xià jià “dī dī chūxíng”App de tōngbào国家网信办：关于下架“滴滴出行”App的通报 [Cyberspace Administration of China: Notification of removing the ‘Didi Chuxing’ app from the app store]. Retrieved April 1, 2023 from http://www.xinhuanet.com/legal/2021-07/04/c_1127621838.htm

Zhou, W. & Zhihang, D. (2023, January 19). Cancer Collaboration Becomes First Overseas Data Transfer Approved Under New Regime. Caixin Global. Retrieved April 1, 2023 from https://www.caixinglobal.com/2023-01-19/cancer-collaboration-becomes-first-overseas-data-transfer-approved-under-new-regime-101991040.html

Annex I



About the authors:

Karin Hess has a background in Sinology, Political Science and Business Administration. As a Swiss national, she has spent two years working amongst others on cyber regulation at the Embassy of Switzerland in Beijing, and advocates for cross-cultural competence in the field of data governance.

Dual Master's Degree in Public Policy at the School of Public Affairs of Sciences Po and Public Administration at the School of Public Policy of the London School of Economics (LSE). Policy stream: Digital, New Technology and Public Policy.

Nicole Grünbaum is an international cooperation advisor with +4 years of experience in digital and open government. She led the Argentine delegation for the G20 Digital Economy Working Group and coordinated the international agenda of the Secretariat of Public Innovation in the Chief of Cabinet's Office.

Master in Public Policy at the School of Public Affairs of Sciences Po. Policy stream: Digital, New Technology and Public Policy

Verónica Arroyo is a Peruvian digital rights activist and lawyer with 4+ of experience working in developing countries around the world. She is CIPP/E certified, and is interested in shaping digital policy of new technology to guarantee privacy, digital security, and the right to be free from discrimination.

Dual Degree Master in Public Policy at the School of Public Affairs of Sciences Po and Master of Global Affairs at the Munk School of Global Affairs and Public Policy of the University of Toronto. Policy stream: Digital, New Technology and Public Policy.

Gustavo Fonseca Ribeiro is a Brazilian lawyer with experience in digital law and policy. He works with Artificial Intelligence and Digital Transformation at UNESCO, in Paris. Previously, he worked in the Technology Team at Baker McKenzie, in Rio de Janeiro. As an affiliate with the Laboratory of Public Policy and Internet (LAPIN), he worked on issues such as data protection, online disinformation, and Internet shutdowns.

Master in Public Policy at the School of Public Affairs of Sciences Po. Policy stream: Digital, New Technology and Public Policy.

About the Digital, governance and sovereignty Chair:

Sciences Po's Digital, Governance and Sovereignty Chair's mission is to foster a unique forum bringing together technical companies, academia, policymakers, civil societies stakeholders, public policy incubators as well as digital regulation experts. Hosted by the School of Public Affairs, the Chair adopts a multidisciplinary and holistic approach to research and analyse the economic, legal, social and institutional transformations brought by digital innovation. The Digital, Governance and Sovereignty Chair is chaired by **Florence G'sell**, Professor of Law at the Université de Lorraine, lecturer at the Sciences Po School of Public Affairs.

The Chair's activities are supported by: