Trade diplomacy implications of data sovereignty & data localization

October 2022

Authors: Dr. Robert Rogowsky, Stephanie Teeuwen, Katarina Zomer
Middlebury Institute of International Studies, Monterey, CA.

KEYWORDS: cross-border data flows, data sovereignty, data localization, European Union, General Data Protection Regulation (GDPR), Japan, Economic Partnership Agreement (EPA), United States of America, China, Regional Comprehensive Economic Partnership (RCEP), India.

Abstract

This study analyzes the diplomatic trade implications of Big Data, data sovereignty and data localization. Globally, an increasing divergence exists within standards and regulation (or lack thereof) of data handling. The main questions discussed in this paper are: what are the diplomatic implications of data sovereignty? In what ways are countries shaping national data regulatory frameworks? And how are these various data localization regulations influencing trade agreements? This paper considers these questions, focusing specifically on the EU, the U.S., and China and how their data regulatory frameworks influence regional trade agreements, including the Economic Partnership Agreement (EPA) between the EU and Japan and the Regional Comprehensive Economic Partnership (RCEP), notably without India. This paper shows that regional governance is taking precedence over global governance. As regionalism and diverging policies increase, it becomes harder to create and maintain a global coherent framework of data regulation. Recognizing this, we therefore recommend setting up an international structure to develop and enforce data regulation.

1. Introduction

Increased digitalization has led to an exponential increase in global e-commerce in recent years.[1] Trade that falls under the heading of e-commerce is estimated to be around 29 trillion USD and will only increase further with rapid digitalization due to the COVID-19 pandemic.[2] Some estimates suggest that e-commerce increased by 50% between 2012 and 2017 (Abendin & Duan, 2021).[3] Data and the (free) flow of data are so essential to digital trade and the rise of e-commerce, that some even refer to data as the 'new oil' and the current moment as the era of Big Data (The Economist, 2017).

Some of the main attributes of Big Data are volume, variety and velocity: volume referring to the sheer amount of data being collected, variety meaning the many types of data and the ways in which it is being collected and stored, and velocity concerning the speed with which data is collected and processed. Though there is no set definition of Big Data, it has been described "as the interplay between these characteristics rather than […] a well-defined and definable object" (Broeders et al., 2017, p. 310).

E-commerce and digitalization increase cross-border data flows, which research shows can increase the Gross Domestic Product (GDP) of a country (Abendin & Duan, 2021). Though the increased flow of data offers vast economic potential to those who can use it, virtually all countries, to various extents and in various forms, are pursuing policies to regulate digital trade and ensure data protection and national sovereignty. The breadth of applicable policies is broad, from antitrust, export subsidies, custom licensing to taxation.[4] A major problem arises in fragmentation

[1] A simple definition of e-commerce is "traditional commercial activities conducted via the Internet" (Kurbalija, 2016, p. 149). Digitalization differs from digitization. Gartner defines: it, digitalization is "the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business." Digitalization moves beyond digitization, leveraging digital information technology to entirely transform a business' processes — evaluating, reengineering and reimagining the way you do business. One would digitize a document but would digitalize the organization's data collection process and workflows.

[2] As IBM, one of the largest technology companies globally, stressed, one of the reasons that we have been able to continue functioning remarkably well during the covid-19 pandemic is exactly because of this flow of free data (Rodriguez & Palmer, 2020).

[3] Data flows and measures of digital trade are imprecise because definitions of what is included as digital trade are still new and evolving, as are data collection mechanisms, and determining if and what economic value to apply to much of the data that is collected and transferred. See also UNCTAD's *Digital Economy Report 2021*, at https://unctad.org/system/files/official-document/der2021_en.pdf.

[4] For an overview of digital policies, see the Activity Tracker of Digital Policy Alert: https://digitalpolicyalert.org/activity-tracker?offset=0&limit=10&period=2020-01-01,2022-10-19.

across a number of policy areas: geo-economic fragmentation as countries enter or fail to enter the digital world, commercial fragmentation as private digital platforms grab dominant market share in national markets, and regulatory fragmentation as countries build their structures individually, creating silos of rules and controls that raise costs of trade (Evenett & Fritz, 2022). As in any new technology and corollary embryonic regulatory regimes, there will be winners and losers within countries and across countries.[5] This paper focuses on only a portion of digital trade—data privacy and security—but the portion that seems of most concern to business and governments and in which fragmentation may impose the most immediate costs.

Businesses collect personal data on individuals on a massive scale and in a vast array of contexts on every aspect of online activity: family and friends networks, browsing and purchase histories, location and physical movements, and a wide range of other personally identifiable information. The growing digitalization of our economy has engendered an exploding industry built on collecting, analyzing, and selling data. Little of it is shared voluntarily. As a result, abuse and potentially unlawful practices may be prevalent.

Algorithms and automated systems analyze the information and sell it into a massive, opaque market for consumer data, using it to place behavioral ads, or leveraging it to sell more products. Some companies fail to adequately secure the consumer data they collect, putting that information at risk to cyber criminals. A growing body of evidence indicates that surveillance-based services may be addictive to children and lead to a wide variety of mental health and social harms.[6] Companies can also make commercial surveillance difficult to avoid. Surveillance can be a condition for service; or a premium paid to keep personal information private. Companies may change privacy terms to expand surveillance. Additionally, companies increasingly employ "dark patterns" or marketing that pushes consumers into sharing personal information.

As more and more people become aware of the invasive nature in which their data are collected and distributed, increased backlash exists against this practice of data mining and more questions arise on who owns what data. Countries see data privacy in different ways: some argue that data belongs to private citizens, others see it as belonging to the government or to private

[5] See also Event & Fritz (2022) and UNCTAD (2021).
[6] Research suggests that teenagers, particularly teenage girls, who spend more than two or three hours daily on social media, suffer from increased rates of depression, anxiety, and thoughts of suicide and self-harm (Twenge et al., 2018; Sampasa-Kanyinga & Lewis, 2015).

companies. According to the EU General Data Protection Regulation (GDPR), for instance, data privacy is a human right, which provides each person the fundamental right to privacy and to control what happens with their data (Abendin & Duan, 2021). Whitman (2004) explains that privacy protection in the EU relies heavily on the dignity of the individual, in contrast to the U.S. perception that privacy is freedom from government interference waived only by national security needs. The rapidly rising economic value of this data creates the intense struggle between free flows of data and privacy protection.

This paper explores the struggle between data sovereignty and data localization. We start by introducing the clash of sovereignty and localization and then look at regulatory frameworks, specifically the EU's GDPR, the Economic Partnership Agreement (EPA) between Japan and the EU, U.S. federal and state data regulation effort, China's regulatory data framework with its influence on the RCEP negotiations, and finally India's data regulation framework and its notable absence from the final RCEP framework. In the end we recommend a framework by which countries can work effectively to share experience, best practices, and regulatory processes to individually and collectively govern this issue of data regulation.

1.1. Data sovereignty

'Sovereignty' gives a state the exclusive power to govern within their state borders. The modern concept of sovereignty can be largely traced back to the 1648 Peace of Westphalia. Recent calls for data sovereignty apply the concept to Big Data. Though it seems new, the idea that "data are subject to the laws and governance structures within the nation where they are collected" has been around since the 1970s (Kuner, 2015, as cited in Potluri et al., 2020, p.2). New technologies generating and collecting massive amounts of data create the public policy conundrum. As Wu posits, "given the vast amounts of data that emerging technologies both use and produce, exploring the way that nation states assert control over data on behalf of their citizens is increasingly necessary for innovation and national security alike" (2021, p. 5). All this data being collected has proven increasingly valuable, for companies about their consumers, but also for countries about their citizens.

As Wu further asserts “digital dominance is increasingly becoming synonymous with economic dominance” (2021, p. 5). As a result, control of data offers both security and economic value. It is not surprising that control by localizing data within the borders of a sovereign country is increasingly of interest.[7]

1.2. Data localization

Following the Snowden revelations and the unavoidable realization that massive amounts of data are being collected, both individuals and states started to consider the implications for privacy, sovereignty, security, and value extraction.[8] Early on, outrage felt by digital rights activists and European citizens generally drove promulgation of the GDPR (Rossi, 2018). Potluri et al. (2020) have identified three types of data localization:

- No restrictions: countries allowing for “free and unconditional cross-border data flows” (p. 3). Some examples of countries with no restrictions on data flows include Ireland and the Netherlands, making these countries attractive places for data centers.
- Less restrictive: countries with some restrictions on cross-border data flows, allowing it “under specific conditions” (p. 3). An example is the United States, calling for localization of data related to national security.[9]
- Highly restrictive: countries with “stringent data localization measures”, like China and India (p. 3). China has the strictest localization measures. Countries within this group tend to have a higher number of digital consumers, thus providing a large market and hence have bargaining power to impose stringent localization requirements.

[7] Note the difference between digital sovereignty and digital autonomy. Whereas sovereignty is from the perspective of a country claiming ownership of its citizens’ data, digital autonomy focuses more on data ownership on an individual level and the ability for individuals to make informed decisions about their data. The European GDPR is a leading example in terms of pursuing digital autonomy, providing specific rights to individuals regarding their personal data ownership.

[8] For an overview of the Snowden revelations, see this webpage put together by Lawfare: https://www.lawfareblog.com/snowden-revelations.

[9] The U.S. tried to include provisions on the free flow of data in trade negotiations during the 80s and 90s, but other nations regarded this as an impediment to their sovereignty, arguing that the U.S. was likely to dominate the realm of e-commerce (Aaronson, 2015).

Countries provide various reasons for imposing data localization measures. Whereas the EU focuses mostly on citizens' individual right to privacy, countries like China and the United States provide national security arguments for data localization measures. India, alternatively, wants to preempt modern day 'data colonialism', arguing that industrialized countries are using data as a means to uphold their economic dominance. In the past two decades, the number of data localization measures has quadrupled.[10]

Data localization measures act as non-tariff barriers to trade.[11] Research indicates that localization of data brings limited economic benefits and instead "can actually stifle innovation and harm growth" (Wu, 2021, p. 15).[12] Localization requirements adversely affect both price and quality of the service provided.[13] The absence of data localization restrictions reduces barriers and the cost of compliance, creating in some sense a digital trading bloc among countries that share localization procedures (Potluri et al., 2020).

2. Regulatory frameworks for Data

Currently, no comprehensive regulatory framework exists to govern cross-border data flows. In this vacuum, countries and regions are forming their own regulatory systems. Given the importance of effective regulation, there have been some global initiatives to manage cross-border data flows and data localization. The World Trade Organization's (WTO) General Agreement on Trade in Services (GATS) of 1995, for example, addressed privacy as an exception within the agreement in situations where countries need to protect "the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of

[10] Francesca Ferracane et al. (2018) have put together a Digital Trade Restrictiveness Index (DTRI) based on data of 100 categories of policy measures in 64 countries. Using this index, Cory & Dascoli (2021) show that increased digital restrictiveness has a negative impact on a country's GDP.

[11] Park (2022) makes the argument that data localization is not only an economic issue, but a human rights issue as well, as it obstructs citizens' rights to choose what entity has control over their data.

[12] Various authors show a negative correlation between data localization measures and GDP, including Bauer et al. (2014), Potluri et al. (2020), and Cory & Dascoli (2021).

[13] Over-The-Top (OTT) services are an exception to this rule. Service providers like Netflix and Hulu prefer to host their data locally, as this increases response time and quality of the streaming service (Potluri et al., 2020).
Note though that this concerns a different type of data. Most localization regulations focus primarily on the data sovereignty of Personally Identifiable Information (PII).

individual records and accounts," so long as this measure was not applied arbitrarily or disguised as a trade restriction on services (Art. XIV).[14]

Since then, the WTO has not been able to update data trade regulations, nor has it seen any specific agreements on data localization.[15] Negotiations regarding this subject started in 2017, with the Joint Initiative on E-Commerce.[16] Though some agreement exists on less controversial issues, including recognizing electronic signatures, WTO members have different views on data localization, based on various political agendas.

2.1. European Union & GDPR

The GDPR, Europe's privacy regulation, came into force in May 2018.[17] The main goals of the GDPR are to create an overarching privacy regulation for the EU and to promote the digital economy by creating more trust by ensuring greater data sovereignty.[18]

The GDPR builds upon prior data protection laws, including the 1995 European Directive on Data Protection and additional national data regulations (Ferracane & Mosi, 2021). Though many concepts in the GDPR are not new, the vast extraterritorial jurisdiction of the GDPR is. The GDPR applies to all EU residents, regardless of citizenship status. It applies to all data being processed within the European Union, regardless of where a company processing this data is incorporated and to all data being processed by companies incorporated in the EU regardless where

[14] Article XIV, GATS, 1995. Related WTO agreements include the GATS and Trade-Related Aspects of Intellectual property Rights (TRIPS).
[15] Other initiatives outside the WTO include the OECD's 1998 Action Plan for Electronic Commerce and the 1998 APEC Blueprint for Action on Electronic Commerce (Kurbalija, 2016).
[16] Though some progress has been made, only about half of the WTO members are participating in these negotiations, with India notably absent. In January 2019, 76 WTO members announced their intention to launch WTO negotiations on e-commerce in a further joint statement. Later that year Canada proposed a concept paper titled "Building Confidence and Trust in Digital Trade" and another in September 2019, along with contributions by other WTO members.
[17] Apart from the GDPR, there are many other recent regulations and directives from the European Union including the "Shaping Europe's Digital Future" strategy, the Digital Services Act, the AI Act, Cybersecurity Act, and NIS Directive, among many other initiatives within the space of data sovereignty.
[18] As Herian describes it, "To be data sovereign is to take control of one's personal digital destiny. This is the tantalizing and powerful idea that the European Union's General Data Protection Regulation (GDPR) […] promotes" (Herian, 2020, p. 156).

the data is being processed (European Commission, n.d.). The reach of the GDPR is both deep and broad.

The GDPR extends its territorial reach through bilateral trade negotiations. When negotiating trade agreements, the European Commission assesses whether the other party has "an adequate level of data protection", meaning protection comparable to the GDPR. As of October 2022, the European Commission has released 14 adequacy decisions, of which 7 apply in countries outside the European continent.[19]

The GDPR emphasizes individual rights, including the right to be forgotten (Art. 17) and the right to data portability (Art. 20).[20] The GDPR recognizes privacy as a human right, concentrating on citizens' individual ownership over their personal data. Whereas data *sovereignty* is inherently state centric, data *autonomy* is focused on individuals being able to make informed decisions about what happens with their data. This contrasts with the idea of China's 'collective sovereignty', according to which the Chinese government claims ownership and control over the data of their citizens.

2.1.1. Economic Partnership Agreement (EPA) of Japan and the EU

The Japanese government is a strong proponent of the free flow of data. At the G20 meeting in Osaka in 2019, Japan called for a "data free flow with trust" as this would optimally "harness the opportunities of the digital economy." The EU, recognising Japan's "adequate level of data protection," in February 2019 entered into an EPA in order to "liberalise and facilitate trade and investment, as well as to promote a closer economic relationship between the Parties" (Art 1.1,

[19] Following the Schrems II decision by the European Commission, the previous EU-U.S. privacy shield was overturned in July 2020. In October 2022, U.S. President Biden signed an executive order for the implementation of an updated EU-U.S. Data Privacy Framework (White House), further removing barriers to cross-border data flows between the two regions.

[20] Article 17 is also known as the right to erasure. According to this right, data should be erased when requested by the data subject. As Herian argues, this right to erasure in some ways makes it harder to take ownership of our own personal data. For instance, as a newly emerging technology, blockchain provides opportunities for individual ownership of data, saved on a distributed and immutable ledger. However, Van Humbeeck (qtd in Herian) argues that "GDPR prohibits us from storing personal data on a blockchain level [since] throwing away your encryption keys is not the same as 'erasure of data'" (p. 164). Since a blockchain is unchangeable, personal data cannot be stored on a blockchain if at the same time one would have to be able to comply with the right to be forgotten.

EU-Japan EPA). The EU and Japan agreed to 'reassess within three years … the need for inclusion of provisions on the free flow of data' (Free flow of data, Art 8.81, EPA).[21]

In August 2022, the European Data Protection Supervisor (EDPS), an independent data protection authority within the EU, concluded that "despite the Adequacy Decision, further negotiations on cross-border data flows are considered to be necessary" (Art. 5.1 Conclusions, EDPS, Opinion 17/2022). The EDPS further stresses that these negotiations should "exclusively concern cross-border data flows between the European Union and Japan" (Art. 2.8, General Remarks, EDPS, Opinion 17/2022). Due to the urgency, complexity, and sensitivity of cross-border data flows and the lack of a multilateral framework, Japan and the European Union have opted for bilateral negotiations, adhering to both Japanese and EU privacy regulations.

2.2. United States

The United States Government (USG) and the individual states have struggled for many years with regulating information and data privacy both generally and in specific cases, such as student information, social security numbers, and medical information.[22] Consumer privacy has rapidly grown in importance in state legislatures. At least 35 states and the District of Columbia introduced or considered almost 200 consumer privacy bills in 2022 alone (National Conference of State Legislatures).

2.2.1. U.S. State Actions

Consumer privacy legislation in states typically targets the collection of data from consumers by commercial entities, online services or commercial websites, including bills related

[21] "The flow of personal data to and from countries outside the European Union is necessary for the expansion of international cooperation and international trade, while guaranteeing that the level of protection afforded to personal data in the European Union is not undermined." (Art. 1, Adequacy decision, EU Commission, January 2019).
[22] For an overview of U.S. state privacy legislation, see the "2022 State Privacy Law Tracker" put together by Husch Blackwel: https://www.huschblackwell.com/2022-state-privacy-law-tracker. For an overview of data privacy laws around the world, see this resource of Allen & Overy sphere: https://www.aosphere.com/aos/dp?gclid=Cj0KCQjw94WZBhDtARIsAKxWG-9bnYoG_oAQJkfz-jI-Sa6HpAQTMZMO3bCNU2DoCZrHkvzwP9ithvIaAn3FEALw_wcB.

to website privacy or children's privacy on the internet, direct-to-consumer genetic testing, Internet Service Provider (ISP) and information/ data broker regulation, and other consumer privacy issues.

Comprehensive (so-called "omnibus") consumer privacy legislation was the most common type of bill being considered—almost 70 bills in at least 25 states and the District of Columbia. Omnibus bills generally regulate the collection, use and disclosure of personal information by businesses and provide an express set of consumer rights for collected data, such as the right to access, correct and delete personal information collected by businesses.

Five states have enacted comprehensive consumer privacy laws:

- California Consumer Privacy Act (CCPA) of 2018 (Cal. Civ. Code §§ 1798.100 et seq.) and California Consumer Privacy Rights Act, 2020 (Proposition 24)
- Colorado Privacy Act (CPA), 2021 S.B. 190 (Effective July 1, 2023)
- Connecticut Data Privacy Act 2022 S.B. 6 (Personal Data Privacy and Online Monitoring) (CCPA) (Effective July 1, 2023)
- Virginia Consumer Data Protection Act (VCDPA), 2021 H.B. 2307 | 2021 S.B. 1392 (Effective Jan. 1, 2023)
- Utah Consumer Privacy Act (UCPA), 2022 S.B. 227 (Effective Dec. 31, 2023)

The enacted state laws consistently define "personal information" or "personal data" broadly. Unlike the CCPA, however, the CTDPA, UCPA, CPA, and VCDPA borrow terms and definitions from the EU GDPR, such as "controller" and "processor," when referring to covered entities and their service providers, respectively, and "personal data." In addition, all the state laws except the UCPA require covered entities to conduct data security assessments for processing activities that present a heightened risk of harm, such as profiling, selling personal data, processing sensitive personal data, and engaging in targeted advertising. Only the CCPA, under the Consumer Right of Privacy Act 2020 (CRPA) provides a right of action for consumers, which is limited to breaches of "personal information".[23] The CPRA extends the CCPA private right of action to data breaches that compromise a username and password and creates a new enforcement body, the California Privacy Protection Agency (CPPA).

[23] As defined more narrowly in a separate data breach notification law than in the CCPA (California Customer Records (2022). Cal. Civ. Code § 1798.80 et seq.).

2.2.2. U.S. Federal Regulations

The U.S. Congress is working to pass comprehensive data privacy and security legislation. In June 2022 the Energy and Commerce Committee voted to pass H.R. 8152, the American Data Privacy and Protection Act (ADPPA) by a vote of 53-2, sending it to the full House for consideration (American Data Protection Act, 2022, H.R.8152).

The ADPPA offers a broader definition of sensitive data than state-level laws, such as income level, voicemails, text messages, calendar information, data relating to a child under the age of 17, and depictions of an individual's "undergarment-clad" private area. State laws tend to focus on health and demographic information. The ADPPA considers sexual orientation information to be sensitive when it is "inconsistent with the individual's reasonable expectation" of disclosure. It is unclear at this point how this will be implemented.

Like the European Union's GDPR, the ADPPA includes a duty of data minimization on "covered entities".[24] There are many exceptions to this rule, including one for using data collected prior to passage "to conduct internal research." ADPPA applies tiered applicability. All commercial entities are "covered entities," but "large data holders" – firms making over $250,000,000 gross revenue and that process either 5,000,000 individuals' data or 200,000 individuals' sensitive data – are subject to additional requirements and limitations. "Small businesses" (those not 'large') have a number of exemptions. Until now, state consumer privacy laws have made applicability an all-or-nothing proposition. All covered entities, however, would be required to comply with browser opt-out signals, such as required in the California Privacy Protection Agency's recent draft regulations. In addition, ADPPA gives individuals a private right of action against covered entities to seek monetary and injunctive relief.

The ADPPA explicitly preempts state privacy laws (albeit explicitly allows CPRA to cover biometric data and retain its breach provisions). Federal law normally sets the regulatory floor for the nation, permitting states to impose more, but not less, rigorous requirements. It makes sense in this case as the globalized nature of the Internet means that any less-stringent state law would become the exception that kills the rule. It does, however, put an additional burden on companies that recently finalized compliance programs to fit state regulations. ADPPA would require covered

[24] The ADPPA borrows this from the Health Insurance Portability and Accountability Act (HIPAA).

entities to minimize collection, processing, and transferring of data to what is "necessary, proportionate, and limited to" their ability to provide or maintain a specific product or service or communicate with the individual.[25]

ADPPA proposes novel requirements for processing and transferring covered data, which includes social security numbers, geolocation information, biometric and genetic information, passwords, aggregated internet search or browsing history, and physical activity information. ADPPA also gives individuals the right to access their data through a downloadable file, obtain the name of any third party holding their data and the purpose, and importantly, to correct any inaccurate data.[26] Four years after the ADPPA becomes law, private citizens can take legal action against violations of ADPPA.

Size matters. ADPPA demands more of "large data holders". For large data holders, the CEO or highest-ranking officer, along with each privacy officer and data security officer at a larger data holder must certify to the FTC that "reasonable" controls are in place to comply with the ADPPA and that reporting structures are in place so certified officers reporting to the CEO design, implement, and enforce compliance and biennial effectiveness reviews.

"Small data holders" - average adjusted gross revenue less than $41 million over the last 3 years that handle data for less than 100,000 individuals annually and generate less than half its revenue from transferring data - need not correct data but can simply delete it. They are exempt from most data security practice requirements, with the exception being the requirement to delete data that is no longer necessary.[27]

The ADPPA defines third-party collecting entities as "covered entity whose principal source of revenue derived from processing or transferring the covered data of individuals that the covered entity did not collect directly from the individuals to which the covered data pertains."

---

[25] Under ADPPA, the Federal Trade Commission (FTC) will establish "necessary, proportionate, and limited to" within one year. Data minimization - a core component of any data privacy program - is one of the more challenging and impactful requirements to implement as it has ripple effects for firms well beyond the privacy or compliance department.

[26] Depending on how an organization is classified (large data holder, covered entity, or a covered entity as described in 209(c)), it will have 30, 60, or 90 days to respond to a request. The majority of states set the time to 45 days with a 45-day extension.

[27] While most state privacy laws exempt nonprofits, ADPPA does not. Many nonprofits likely will qualify as small data holders.

Third-party collecting entities must (i) place a clear notice on their websites or apps stating it is collecting data on behalf of another organization, (ii) establish measures that allow for the auditing of covered data, and (iii) provide the required information for the Third-Party Collecting Entity Registry.

2.2.2.1. Federal Trade Commission (FTC)

The FTC commenced in August 2022 an Advance Notice of Proposed Rulemaking to regulate commercial surveillance and data security practices and determine rules necessary to protect people's privacy and information.[28]

In the last two decades, the FTC has brought hundreds of enforcement actions against companies for privacy and data security violations.[29] These include cases involving the sharing of health-related data with third parties, the collection and sharing of sensitive television viewing data for targeted advertising, and the failure to implement reasonable security measures to protect sensitive personal data such as Social Security numbers.

---

[28] In 1975, Congress passed the Magnuson-Moss Warranty— Federal Trade Commission Improvement Act (the "Magnuson-Moss Act"). That Act made explicit the Commission's authority to prescribe rules prohibiting unfair or deceptive trade practices. It also set out steps for doing so, including providing informal oral hearings with a limited right of cross examination, which were consistent with best practices of that time. In the decade following its passage, the Magnuson-Moss Act was viewed as "substantially increasing the agency's rulemaking powers."
Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975).
4 Id. at sec. 202 (adding § 18(c) of the FTC Act) (Walters, 2022).

[29] The FTC is authorized to protect against 'unfair' practices by Section 5 of the FTC Act, (15 U.S.C 45(n)) if (1) it causes or is likely to cause substantial injury, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or competition. A representation, omission, or practice is deceptive under Section 5 if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers—that is, it would likely affect the consumer's conduct or decision regarding a product or service. Under the statute, this broad language is applied to specific commercial practices through Commission enforcement actions and the promulgation of trade regulation rules. In addition to the FTC Act, the Commission enforces a number of sector-specific laws that relate to commercial surveillance practices, including: the Fair Credit Reporting Act, which protects the privacy of consumer information collected by consumer reporting agencies; the Children's Online Privacy Protection Act ("COPPA"), which protects information collected online from children under the age of 13; the Gramm-Leach-Bliley Act ("GLBA"), which protects the privacy of customer information collected by financial institutions; the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act, which allows consumers to opt out of receiving commercial email messages; the Fair Debt Collection Practices Act, which protects individuals from harassment by debt collectors and imposes disclosure requirements on related third-parties; the Telemarketing and Consumer Fraud and Abuse Prevention Act, under which the Commission implemented the Do Not Call Registry; the Health Breach Notification Rule, which applies to certain health information; and the Equal Credit Opportunity Act, which protects individuals from discrimination on the basis of race, color, religion, national origin, sex, marital status, receipt of public assistance, or good faith exercise of rights under the Consumer. Credit Protection Act and requires creditors to provide to applicants, upon request, the reasons underlying decisions to deny credit. See Federal Register (2022).

The FTC is concerned that enforcement alone has weaknesses, specifically that the agency is not empowered to seek financial penalties for initial violations of the FTC Act. However, it believes that rules establishing clear privacy and data security requirements across the board will provide the Commission authority to seek financial penalties for first-time violations.[30]

2.2.3. U.S. negotiations with TikTok

Chinese-owned TikTok, one of the world's most popular social media apps, has become a symbol of the technology and digital data war between Beijing and Washington. Lawmakers and regulators have repeatedly raised concerns about TikTok's ability to protect the data of American users from Chinese authorities. In June 2022, the New York Times reported that employees of ByteDance, TikTok's parent company, had access to TikTok's U.S. data (McCabe). The Trump Administration unsuccessfully tried to force ByteDance to sell TikTok to an American company in 2020 and threatened to block the app.[31]

The Biden Justice Department, assertively supported by the Treasury Department, is negotiating with TikTok to resolve the national security concerns. TikTok seeks to both remain owned by ByteDance and operate in the United States by negotiating changes in its data security and governance. Additionally, TikTok has been negotiating with representatives for the Committee on Foreign Investment in the United States (CFIUS), a group of federal agencies that reviews investments by foreign entities in American companies, to resolve concerns that the app puts national security at risk (Wang & Shepardson, 2022). CFIUS must approve any agreement, which potentially could rise to the President. The Treasury Department, which leads the group, has stated its commitment "to taking all necessary actions within its authority to safeguard U.S. national security." TikTok, in turn, has committed "to fully satisfy all reasonable U.S. national security concerns" (Hirsch et al., 2022).

[30] Some commissioners opposed the Rulemaking, arguing that the FTC should wait for the ADPPA to be passed before acting.

[31] Trump ordered ByteDance to sell the app or risk being blocked from Apple's and Google's app stores in 2020. The Chinese company appeared to reach an agreement to sell part of TikTok to Oracle, the American cloud computing company. But the deal never closed, and a federal court ruled against Mr. Trump's attempt to block the app. The Biden Administration rolled back Mr. Trump's demand that TikTok be blocked and set out to develop a policy toward the app and others owned by foreign entities.

Negotiations between CFIUS and TikTok evolve around complex technical questions about data handling. TikTok reportedly would make changes to three main areas:

1. TikTok would store its American data solely on U.S. servers, probably run by Oracle, instead of its own servers in Singapore and Virginia.
2. American cloud computing company Oracle would monitor the algorithms used by TikTok that determine the pushed content.
3. TikTok would create a board of security experts to oversee U.S. operations and report to the U.S. government (Hirsch et al., 2022).

The Biden Administration is not without its own internal debate: scaling back costly U.S. tariffs on Chinese imports and more open trade versus closer and tighter scrutiny of all commercial ties with China. Biden seems to be trying to balance between them.

The Biden administration issued an executive order that directed CFIUS to focus on whether deals would expose U.S. data to foreign adversaries (White House, October 2022).[32] It issued another in October 2022 tightening Signals Intelligence Activities.[33] In addition, the White

[32] The E.O. directs the Committee to consider five specific sets of factors:
1. The resilience of critical U.S. supply chains that may have national security implications, including those outside of the defense industrial base.
2. U.S. technological leadership in areas affecting U.S. national security, including but not limited to microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies.
3. Industry investment trends that may hurt U.S. national security.
4. Cybersecurity risks that threaten to impair national security.
5. Risks to U.S. persons' sensitive data, specifically whether a covered transaction involves a U.S. business with access to U.S. persons' sensitive data, and whether the foreign investor has, or the parties to whom the foreign investor has ties, have sought or have the ability to exploit such information to the detriment of national security, including through the use of commercial or other means.

[33] Executive Order on *Enhancing Safeguards for United States Signals Intelligence Activities* directing the steps that to implement the U.S. commitments under the European Union-U.S. Data Privacy Framework (EU-U.S. DPF) announced by President Biden and President von der Leyen in March 2022 (White House, March 2022). The E.O limits data collection, regardless of nationality or country of residence, to "defined national security objectives" and only when "necessary to advance a validated intelligence priority and only to the extent and in a manner proportionate to that priority." The E.O. mandates stricter handling requirements for personal information collected through signals intelligence activities and extends the responsibilities of legal, oversight, and compliance officials to ensure that appropriate actions are taken to remediate incidents of non-compliance. The U.S. Intelligence Community shall update their policies and procedures to reflect the new privacy and civil liberties safeguards. In addition, it requires a multi-layer mechanism for binding review and redress of claims. In particular, the Civil Liberties Protection Officer in the Office of the Director of National Intelligence (CLPO) can determine if the E.O.'s enhanced safeguards

House is considering additional Executive Orders to (1) address American firms investing in Chinese firms and (2) give the government more power to monitor and control apps that, like TikTok, could leak data to a foreign power. The resolution of the TikTok controversy should provide a roadmap for future cases posed by Chinese firms in the U.S. market and especially those gathering and using Big Data.[34]

2.3. China

Since the passage of China's Cybersecurity Law in 2017, the Chinese government has created a series of laws and regulations focused on controlling, sharing, and commercializing data (Erie & Streinz, 2021).[35] China's national data and privacy protection system – in contrast to the GDPR's emphasis on individual autonomy – is one of collective sovereignty, which emphasizes national security, and restricts international trade and the free flow of information to varying degrees. The growth of China's digital economy has led to government support of data and cyber sovereignty, thereby asserting the legitimacy of governmental control over all data and data flows (Erie & Streinz, 2021). Data sovereignty refers to the legal notion that data is subject to the rules and regulations in the jurisdiction where it is harvested, processed, sold, and consumed. Cyber sovereignty, a phrase used by the Chinese Communist Party (CCP) to justify their strong control over cyberspace, data, and networks within the country, allows the CCP to create a "Chinese Internet", monitor and regulate their own citizen's data, influence their adversaries' data, and hold network power (Sherman, 2019).[36]

From one perspective, China's position can appear to be an economically motivated decision to control production and engage in international supply chains. By dominating Big Data,

---

or other applicable U.S. law were violated and set the appropriate remediation; binding subject to review by a new Data Protection Review Court ("DPRC") to be set up by the Department of Justice.

[34] China has stated their ambition to be a market leader in the fourth industrial revolution, or Digital Revolution as it is also known. *Made in China 2025* demonstrates China's deep desire to lead in the Digital Revolution, where data is a key factor of production as Big Data, cloud computing, and other emerging technologies are driving global supply chains (McBride & Chatzky, 2019).

[35] For a recent article on Chinese regulations of cross-border flows of data, see Huang & Shen (2022).

[36] "Network power" is the ability to control data and influence outcomes, which is increasingly important as interoperable networks grow and connect.

data sovereignty, and data localization, the CCP can maintain control over information and any expression of dissent.[37] In contrast to the U.S.' belief in the free flow of data, China's authoritarian cyber sovereignty stance and its adept application of it for homeland security, appeals to authoritarian or illiberal governments, such as Russia, Vietnam and Myanmar (Sherman, 2019). Cyber sovereignty and data localization policies permit governments to seize data for national security reasons, jeopardizing civil and intellectual property rights.

Recent Chinese digital regulations, including the Personal Information Protection Law (PIPL), the Data Security Law (DSL), the Measures of Security Assessments for Data Export, and the Regulations on Network Data Security Management, represent the most recent links in a chain of digital privacy and information control laws that promulgated to protect consumers, and are also ensconced in a national security framework that can serve other state purposes, such as surveillance. Yet, concerns about the Chinese government's access to, and control of Big Data goes beyond espionage or surveillance. As the U.K. MI6 Chief Richard Moore stated, allowing one country to gain access to critical data about another society erodes national sovereignty as countries lose control over that data (Bowden, 2021).

The PIPL, which took effect on November 1, 2021, is China's first comprehensive law designed to regulate online data and protect personal information. It sets forth rules for processing personal information and defining individual rights with respect to one's digital footprint. Drawing upon the GDPR, the PIPL regulates how businesses interact with personal data and lays out rules and definitions for the collection and commercial exploitation of personal information (Zhu, 2022). Key provisions of the PIPL involve international trade, specifically cross-border data flows. Article 53 states that Personal Information Processing Entities (PIPEs) outside of China's borders must establish an organization or individual within China to handle matters relating to the collection of personal information from Chinese nationals. Article 54 mandates regular audits of compliance with the PIPL. Through these two provisions, China affords itself access to international data flows of businesses that possibly infringe the sovereignty of companies. Article 41 mandates that information stored in China may not be provided to a foreign government without the consent of the Chinese government (Creemers & Webster, August 2021). The PIPL has resulted in the implementation of a regulatory framework that, while created to protect the personal

[37] This control can also be called cyber sovereignty; see U.S.-China Economic and Security Review Commission

information of Chinese citizens, also consolidates government oversight and control of the digital economy on an international scale.

China's Data Security Law (DSL) is the government's first attempt to comprehensively regulate data by strengthening the national security related data storage and transfer infrastructure.[38] The DSL has a broader scope and applies to all entities inside and outside China with data that could "impair the national security, public interests, and people's legitimate interests in China" (Erie & Streinz, 2021, p. 30). Article 21 directs the Cybersecurity Administration of China (CAC) to establish a system of protecting data according to its proximity to national security and public interest (Creemers & Webster, June 2021). As with many regulatory systems in China, the law calls for national, provincial, and municipal mechanisms ensuring data security. The national and local branches of the CAC determine specific 'catalogs' of important data; companies that handle it are subject to more stringent checks (Creemers & Webster, June 2021).

The CAC sorts data into two categories, "important data" or "core data," depending on its proximity to China's national security apparatus. The definition of "important data" is vague; the DSL states that industry specific catalogs of important data will be developed "according to the risk those data pose to national security, economic security, and people's livelihoods if compromised" (Douglas & Feldshuh, 2022).[39] The label is likely to be heavily contingent on the capacity of local governments to develop the definition of "important data" for industries in their jurisdiction.[40] Nonetheless, the DSL requires heightened levels of security protection, that data be localized, and a risk assessment be completed prior to international transfer of important data (Douglas & Feldshuh, 2022). Core data, on the other hand, can be more easily defined as classified information related to China's military, government, and state secrets, and thus has much stricter regulations due to its relevance to national security.[41] The DSL does not define the exact parameters of core data, yet foreign businesses cannot handle such data (Douglas & Feldshuh, 2022). The creation of hierarchical categories based on proximity to sensitive state subjects and protected personal domains with differing rules for each level of data is muddied by the lack of clarity for the benchmarks that separate each level. This seemingly deliberate ambiguity grants

[38] The DSL is a relatively new regulation that went into effect on September 1, 2021.
[39] Douglas & Feldshuh, 2022 page 5.
[40] Z. Tomatz (personal communication, August 15, 2022).
[41] idem.

regulators the ability to seize data, conduct investigations, and stem international data flows as required by the law, but also as deemed necessary to fulfill other state objectives. Vague data localization regulations with serious penalties raise foreign businesses' costs, disrupt global systems, and limit the types of goods and services that can enter. A 2021 Congressional Research Service study stated that computing costs in markets with localization requirements, such as China, can be 30−60% higher than in open markets (Douglas & Feldshuh, 2022).

China's current vague and restrictive national security focused approach to data governance makes it likely that they will demand national security exceptions in any trade agreements. Traditionally, China has refused to negotiate trade rules around data governance and data flows. China refused to sign onto the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules (APEC CBPR), citing that it serves the interests of the U.S. (Cory, 2019). Yet, China has become interested in joining new trade agreements where countries are just deciding on digital trade rules and digital economic governance. On the other hand, in 2021, China applied to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA).[42] Accession to either would require China to change their domestic laws and regulations on data flows; a far stretch for China. One concern is that China wants an insider advantage from joining these agreements to mold them in ways supporting Chinese influence.

2.3.1. The Regional Comprehensive Economic Partnership (RCEP)

RCEP, launched January 2022, includes both broad provisions on protecting data flow and data localization, and broad exceptions founded in national security concerns.[43] RCEP data flow provisions are not subject to the normal dispute settlement procedure, thus making them unenforceable and weaker than provisions in the WTO General Agreement on Trade in Services (RCEP, Chapter 12 Electronic Commerce). Both agreements have exceptions where any member is allowed to adopt "any measure that it considers necessary for the protection of its essential security interests." The exceptions also specifically state that these measures "shall not be disputed

[42] It must be noted that the U.S. is not involved in these agreements.
[43] RCEP includes Australia, Brunei, Cambodia, China, Indonesia, Japan, Laos, Malaysia, Myanmar, New Zealand, Philippines, Singapore, South Korea, Thailand, and Vietnam, encompassing an area of 2.3 billion people (ASEAN, 2022; Schott, 2022).

by other Parties;" thus exceptions are self-determined and not subject to legal challenge. However, Articles 12.14 and 12.15 outline that members are not allowed to misuse the exceptions to enact discriminatory and camouflaged trade barriers. China's participation in the RCEP, the world's largest Free Trade Agreement (FTA), suggests its evolving approach to data and digital trade as a method to greater regional influence as ASEAN countries build their data governance policies.[44]

China, among others, is likely to sign Agreements related to data and digital trade if it can get broad self-assessed exceptions for national security reasons that allow it to circumvent the intended impact of the new regulations. Stronger standards with fewer exceptions would require significant coordination among, and hard bargaining by, liberal democracies to achieve a globally coherent and enforceable framework on data regulation at the WTO.

2.4. India

Engaged in the RCEP negotiations from 2011-2019, India ultimately walked away. The implications for India are uncertain, and the reviews mixed.[45] Nonetheless, India may have influenced the direction of the RCEP in the negotiations, thus playing a (perhaps limited) role in norm setting.

---

[44] RCEP's chapter 12 on electronic commerce indicates what China, the RCEP's dominant member state, is willing to accept. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership's (CPTPP) chapter 14 on e-commerce is essentially the digital chapter of USMCA. Like CPTPP, rules do not apply to government procurement or information by or for governments. RCEP has language similar to CPTPP for cooperation, paperless trading, electronic authentication and electronic signature, online consumer protection, personal information protection, unsolicited commercial electronic messages, domestic regulatory framework, customs duties and cybersecurity. However, in covering the location of computing facilities, cross-border transfer of information by electronic means, source code and dispute settlement, RCEP renders empty its "protection" of cross-border digital trade and data flows. Chapter 12 allows member states to impose whatever national regulatory restrictions they wish, as long as it is consistent with national treatment. Moreover, discrimination can occur because RCEP's dispute settlement mechanism does not apply to chapter 12. Hence, if members cannot resolve disputes through consultation, it goes to the Joint Committee (ministerial level) for further discussion but with no authority to impose a decision. Regarding location of computing facilities, Chapter 14 mirrors CPTPP's language prohibiting such requirements but adds a critical footnote affirming that the need for any exceptions "shall be decided by the implementing Party." Anything is legitimate if a Party says it is legitimate. Adding for emphasis, permission for "any measure that [a Party] considers necessary for the protection of its essential security interests;" and "Such measures shall not be disputed by other Parties." (The CPTPP permits restrictions based on a legitimate public policy objective if it does not impose restrictions 'greater than are required to achieve the objective."). RCEP's restrictions on cross-border transfer of information by electronic means follows the language above. CPTPP states that "No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory." RCEP members are free to require such transfer or access as a condition for market access. In sum, RCEP's e-commerce chapter is built on the CPTPP's framework, but adds and subtracts language to carve out broad paths to control digital trade and data.

[45] See for example Erken & Every (2020) and Gupta & Ganguly (2020).

Similar to the *Made in China 2025* plan, India also aspires to global leadership, especially in technology. Following India's Gandhian struggle for self-reliance and self-sufficiency *atmanirbhar Bharat*, Modi formalized the *Make in India* strategy when he became prime minister in 2014. A key part of this strategy is to become an exporter of telecom technology by 2023 (Bhargava, 2022).

With over $200 billion in revenues, the Information and Communication Technology (ICT) sector currently accounts for about 13% of India's GDP.[46] Given the size of India's IT exports, one would expect the Indian government to be a strong proponent of a free flow of data, as this could greatly benefit the Indian economy. However, as Parsheera points out, "India […] holds a distinct strategic viewpoint on cross-border data flows" (2022, p.59).

New Delhi is wary of joining either the 'West' with the U.S. and Europe or the 'East' with China in terms of data regulation, stemming from India's long history of non-alignment. By leading in the export of telecom technology, India would avoid being at the mercy of either American or Chinese companies. Part of the strategy is to reject 'data colonialism,' a term coined by Couldry & Mejias to account for 'a new stage of capitalism' in a time of Big Data (2019, p. 336). Indian businessmen are calling upon Prime Minister Modi to promote data sovereignty by ensuring that Indians themselves reap the economic benefits of their data (Vila Seoane, 2021). The benefits of data and digital development have been distributed in an uneven manner, with private corporations taking most profits. A report by the Carnegie Endowment for International Peace indicated that "the revenues of six major U.S.-based technology companies in 2021 exceeded $1.4 trillion, which is more than forty times the size of India's estimated benefits from digital trade in 2019" (Parsheera, 2022, p. 50). Given this vast inequality, voices within India have been calling for more stringent data localization measures, as a "defense against data colonialism" (Vila Seoane, 2021, p. 1739).

To ensure data sovereignty, the Indian government has been working on a "comprehensive legal framework for digital economy" (Bhargava, 2022). Following a Supreme Court decision in 2017 acknowledging privacy as a fundamental right, and a landmark case in 2018 that arose following concerns about extensive government surveillance, India had been working for three

[46] According to data of the International Trade Administration (2021), within the U.S. Department of Commerce.

years on the ‘Personal Data Protection Bill, 2019’ (Matthan & Ramans, 2022). In August 2022, the Indian government unexpectedly abandoned this bill, stressing that “it should be in tune with … modern times” (Bhargava, 2022). Though there were concerns with the 2019 Bill regarding the government’s far-reaching control over personal data, as the executive director of the Internet Freedom Foundation Apar Gupta said in a New York Times article, “It’s not about getting a perfect law, but a law at this point” (Yasir & Deep Singh, 2022).

3. Recommendations: an international structure to develop and enforce data regulation

Echoing Gupta’s sentiment, it is crucial to take action on regulation concerning the cross-border flow of data. International regulatory cooperation is hard though. Easy in theory but exceedingly difficult in practice, especially with a contentious and fast-changing topic like data regulation. This difficulty was the crux of both the ambition and the failure of the Transatlantic Trade and Investment Partnership (TTIP). Regulatory cooperation is a multi-step process of integrating different countries’ sovereign regulatory regimes. Free trade agreements typically seek a form of harmonization of national regulations, or at least a mutual recognition in which compliance with one country’s requirements is sufficient to meet the other’s requirements, as is the case with adequacy decisions on data regulations of the European Commission. Most regulatory integration provisions are in fact roadmaps for prescribed collaboration, discussion, sharing best practices and agreements to enforce one’s own laws diligently, and share information in cross-border enforcement efforts.

States that are determined to succeed in the struggle of sovereignty over personal data protections, which are aimed at transnational economic activity, must take aggressive steps toward agreements that foster collaboration, legal and regulatory consistency, and cooperative enforcement. The regulatory agencies in collaborating countries must share information, experiences and best practices. In addition, respective regulators must actively seek to align their domestic regulations and enforcement, recognizing that doing so will require extensive, long-term

negotiations that may never succeed. However, success is found not in total harmonization, but in asymptotically converging on effective alignment of regulations and enforcement.

3.1. Proposed steps toward effective regulatory cooperation

Formal Agreements on Regulatory Cooperation: National regulatory authorities, including both legislators and executive branch officials, agree to exchange detailed information on legislation, implementing regulation and enforcement actions. As these would not be intended to negotiate any form of mutual recognition or imposed harmonization, they could easily be constructed to share information for collaboration to improve individual and dual enforcement.

The transnational nature of economic interaction in which data privacy and security must be protected ineluctably pushes cooperating nations to wrestle with conjoined enforcement. To avoid the political traps of pushing for high-level harmonization (e.g., TTIP), data privacy and security can most effectively be kept at the technical expert level. We therefore recommend the following:

1. Set up a regulatory council consisting of high-level technical officials of relevant regulatory agencies in participating nations.[47] The G-7 would be a logical first group to establish both the structure for rigorous analysis of best practices and negotiating collaborative solutions at the technical level. It can and should expand to other like-minded and willing nations as the model gains experience.

[47] Useful examples are easily found. The United States and Mexico recently relaunched the U.S.-Mexico High-Level Economic Dialogue (HLED) coordinating bilateral efforts to promote innovation; promoting investment in entrepreneurs and SMEs (Office of the United States Trade Representative, 2021). The HLED advances strategic economic and social dialogue fostering regional economic growth, job creation, investment in human capital, and reducing inequality and poverty. The HLED structure offers a general framework for bilateral cooperation. In early 2022, the United States and Japan created the new ministerial-level Economic Policy Consultative Committee (the Economic "2+2"), to track and drive economic cooperation and to strengthen the rules-based economic order (White House, January, 2022). In the inaugural meeting in mid-2022, Ministers reviewed ways to defend workers, companies, and investors against the harms of unfair, anti-competitive, and non-market policies and practices. The Ministers also advanced shared objectives under the US-Japan Competitiveness and Resilience (CoRe) Partnership and committed to countering threats to economic security, resilience, and diversification of critical supply chains, promoting and protecting critical and emerging technologies, export controls, and the illicit diversion of technology critical for weapons development.

2. Create a small Secretariat to establish an international agency presence to ensure formal institutional collaboration and to push the agenda and monitor and support implementation.[48]

   a. The Secretariat would be a focal point for data gathering, sponsoring and disseminating research, and coordinating (and recruiting) non-participating nations.

   b. Coordinate and manage the broad array of stakeholders who should be included in effective analysis and consideration of 'best practices' and collaborative implementation and training.

   c. Notably, the Secretariat would be most helpful in creating paths for negotiation when substantial disagreements occur between nations in enforcement actions.

The TTIP negotiations proved unsuccessful as the negotiation ambitions were too high, skipping the critical 'working together' foundation of effective diplomacy and instead aiming for enforceable regulations. The proactive efforts across almost all nations to face the rising problem of data regulation testifies to the broad recognition of a mutual problem. Solid strategic leadership

[48] USMCA Chapter 19 sets out the provisions for all Digital Trade among parties, but for government procurement. It bars customs duties, fees, or other charges on or in connection with digital products transmitted electronically among Parties. It requires strict National Treatment but for government subsidies or grants (loan, guarantees or insurance). Parties agree to (i) maintain a legal framework based on the *UNCITRAL Model Law on Electronic Commerce 1996*, (ii) avoid unnecessary regulatory burden and (iii) facilitate public input to its laws and regulations. Parties will accept electronic signatures and a trade administration document submitted electronically as the legal equivalent of the paper version of that document. Parties agree to protect consumers from fraudulent or deceptive commercial activities by maintaining laws against online fraudulent and deceptive commercial activities and to coordinate cross-border digital trade in ways that enhance consumer welfare. The legal frameworks will build on shared best practices, including those proffered by the *APEC Privacy Framework* and the *OECD Guidelines*. To protect domestic and cross-border flows of personal information, Parties will adopt non-discriminatory practices in protecting users of digital trade and publish information on the personal information protections it provides, including steps for consumers to pursue a remedy and for an enterprise to comply with legal requirements. Recognizing different legal approaches to protecting personal information, each Party will promote compatibility, including exchange information and other suitable arrangements to promote compatibility between them, e.g. *APEC Cross-Border Privacy Rules* system. Any restrictions must be necessary for a legitimate public policy objective and must be the least burdensome to trade possible. No Party will require any person or business to use or locate computing facilities within a Party or require source code or algorithms to be provided as a condition of entry (except as required for law enforcement actions). To enhance cross-border cooperation Parties agree to regular dialogue on all relevant regulatory and enforcement issues, including cybersecurity by collaboration and cooperation on detection and enforcement. Parties agree to treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to that information unless the supplier or user created the information. Suppliers/ users can still restrict harmful or objectionable content. Parties shall cooperate to expand access to and use of government information, to generate business opportunities, especially for SMEs.

to bring officials and experts together to share and study experiences, determine best ways to work together toward mutual benefit, and to study experience and theory (but with no mandate and little pressure to impose one nation's rules, or even agreed upon best regulatory practices), should provide a constructive program for effective collaborative protections.

4. Conclusion

There is no globally accepted data sovereignty framework, nor are there comprehensive binding multilateral agreements and laws about privacy protection, data localization, or cross-border data flows. Countries vary in their data policies, some promoting data localization while others emphasize the importance of free flow of data and its impact on the global economy. These country specific policies have restricted international trade and e-commerce. Several international organizations have attempted to develop best practice guidelines on privacy and cross-border data flows but differing cultural values and interests have made it hard to come to an agreement. While a multilateral regulatory system has not come about, regional systems have thrived. The EU, through the GDPR, established rules emphasizing individual privacy. China established rules focused on national security concerns. The U.S., unlike the EU or China, has based its policies on creating a balance between trade, privacy, and security.

Data will only become more important as new and emerging technologies increase the importance of free cross-border data flows. Given the differing interests within the digital sphere, a multilateral agreement reached within the WTO is improbable. In the absence of multilateral agreements, far reaching national regulations regarding Big Data, data sovereignty, and data localization will grow, stifling international commerce. Finding a global consensus on how to balance cross-border data flows and privacy protection is key in maintaining trust in the digital environment, protecting the public core of the Internet, and advancing trade.

As countries increasingly implement different data sovereignty frameworks, this affects the Internet's technical infrastructure, potentially leading to a further fragmentation of the Internet: a so-called splinternet. It is imperative that the data regulatory framework be one that is based on values, respects sovereignty and accommodates its fundamentally transnational nature.

References

Aaronson, S. (2015). Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. *World Trade Review, 14*(4), 671-700. doi:10.1017/S1474745615000014

Abendin, S., & Duan, P. (2021). Global E-Commerce Talks at the WTO: Positions on Selected Issues of the United States, European Union, China, and Japan. *World Trade Review, 20*(5), 707-724. doi:10.1017/S1474745621000094

Allen & Overy sphere (n.d.). *Global Data Privacy Laws: Analysis of international privacy laws, curated by experts.* https://www.aosphere.com/aos/dp?gclid=Cj0KCQjw94WZBhDtARIsAKxWG-9bnYoG_oAQJkfz-jI-Sa6HpAQTMZMO3bCNU2DoCZrHkvzwP9ithvIaAn3FEALw_wcB

American Data Privacy and Protection Act (2022). H.R.8152. House - Energy and Commerce Committee, U.S. Congress. https://www.congress.gov/bill/117th-congress/house-bill/8152/text

Asia-Pacific Economic Cooperation (APEC) Privacy Framework, December, 2005, https://www.apec.org/publications/2005/12/apec-privacy-framework

Asia-Pacific Economic Cooperation (APEC) (2021, October). What is the Cross-Border Privacy Rules System. https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system

Association of Southeast Asian Nations (ASEAN) (2022, January 1). *RCEP Agreement enters into force*. https://asean.org/rcep-agreement-enters-into-force/

Bauer, M., Lee-Makiyama, H., Van der Marel, E., & Verschelde, B. (2014). The costs of data localisation: Friendly fire on economic recovery. *European Centre for International Political Economy (ECIPE), 3.* http://hdl.handle.net/10419/174726

Bhargava, Y. (2022, August 28). *Draft legislation will be out for consultation soon, says Union Communication Minister*. The Hindu. https://www.thehindu.com/opinion/interview/ashwini-vaishnaw-interview-new-draft-data-protection-bill-to-be-out-soon-for-consultation/article65822798.ece

Bowden, G. (2021, November 30). *MI6 boss warns of China 'debt traps and data traps'*. BBC. https://www.bbc.com/news/uk-59474365

Broeders, D., Schrijvers, E., Van der Sloot, B., Van Brakel, R., De Hoog, J., & Hirsch Ballin, E. (2017, June). Big Data and security policies: Towards a framework for regulating the

phases of analytics and use of Big Data. *Computer law & security review, 33(3)*, 309-323. http://dx.doi.org/10.1016/j.clsr.2017.03.002

California Consumer Privacy Act (2018). Cal. Civ. Code § 1798.100 et seq. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

California Customer Records (2022). Cal. Civ. Code § 1798.80 et seq. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82

California Consumer Privacy Rights Act (2020). Proposition 24, Section 8 of Article II of the California Constitution. https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf

Canada (2019, May 9). *Joint statement on electronic commerce*. Concept paper: Building confidence and trust in digital trade. https://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/other-autre/statement-concept-ecom-declaration-reflexion.aspx?lang=eng

Canada (2019, September 4). *WTO Joint Statement Initiative on Electronic Commerce*. Concept Paper: Preventing the use of Personal Information from being used for the Discrimination or Persecution of Natural Persons. https://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/other-autre/statement-concept-ecom-declaration-reflexion-09.aspx?lang=eng

Colorado Privacy Act (2021, July 7). Senate Bill 21-190, Colorado Revised Statutes, (part 13). Effective July 1, 2023. https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

Connecticut Data Privacy Act (2022, February). An act concerning personal data privacy and online monitoring. Effective July 1, 2023. https://www.cga.ct.gov/2022/amd/S/pdf/2022SB-00006-R00SA-AMD.pdf

Cory, N. (2019, May 9). Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules. *Information Technology & Innovation Foundation.* https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital/

Cory, N., & Dascoli, L. (2021, July 19). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. *Information Technology & Innovation Foundation.* https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

Couldry, N., & Mejias, U.A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media, 20*(4), 336-349. https://doi.org/10.1177/1527476418796632

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (2018). *Chapter 14: Electronic Commerce*. https://www.international.gc.ca/trade-

commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng

Creemers, R., & Webster, G. (Ed.). (2021, June 29). *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*. DigiChina, Stanford University. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

Creemers, R., & Webster, G. (2021, August 20). *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*. DigiChina, Stanford University. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Digital Policy Alert. *Activity Tracker*. https://digitalpolicyalert.org/activity-tracker?offset=0&limit=10&period=2020-01-01,2022-10-19

Douglas, A., & Feldshuh, H. (2022, April). How American Companies are Approaching China's Data, Privacy, and Cybersecurity Regimes. *The U.S. China Business Council.* https://www.uschina.org/sites/default/files/how_american_companies_are_approaching_chinas_data_privacy_and_cybersecurity_regimes.pdf

Erie, M. S., & Streinz, T. (2021). The Beijing Effect: China's Digital Silk Road As Transnational Data Governance. *New York University - Journal of International Law and Politics.* https://ssrn.com/abstract=3810256

Erken, H., & Every, M. (2020, December). Why India is wise not to join RCEP. *RaboResearch - Economic Research, Rabobank.* https://economics.rabobank.com/publications/2020/december/why-india-is-wise-not-to-join-rcep/

Evenett, S. J., & Fritz, J. (2022. June 28). Emergent Digital Fragmentation: the Perils of Unilateralism. *Centre for Economic Policy Research (CEPR Press).* https://www.hinrichfoundation.com/research/wp/digital/emergent-digital-fragmentation-the-perils-of-unilateralism/

European Commission. (n.d.). *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection.* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Commission. (n.d.). *Who does the data protection law apply to?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en

European Data Protection Supervisor (2022). *Opinion 17/2022.* https://edps.europa.eu/system/files/2022-08/22-08-09_edps_opinion_eu_japan_en.pdf

EU-Japan Economic Partnership Agreement, February 1, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0192#document2

Federal Register (2022, August 22). *Trade Regulation Rule on Commercial Surveillance and Data Security*. https://www.federalregister.gov/d/2022-17752/p-98

Ferracane, M. F., Lee-Makiyama, H., & Van der Marel, E. (2018). Digital Trade Restrictiveness Index. *European Centre for International Political Economy (ECIPE).* https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

Ferracane, M.F., & Mosi, L. (2021). What kind of rules are needed to support digital trade? In B. Hoekman, X. Tu, & D. Wang (Eds.), *Rebooting Multilateral Trade Cooperation: Perspectives from China and Europe* (pp. 153-176). Centre for Economic Policy Research (CERP) Press. https://cepr.org/publications/books-and-reports/rebooting-multilateral-trade-cooperation-perspectives-china-and

G20 Osaka Summit 2019. (2019). *G20 Osaka Leaders' Declaration.* https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html

Gallagher, B. (2020, December 21). Will the U.S. Adopt a Nationwide Data Privacy Law Similar to GDPR? *IS Partners LLC.* https://www.ispartnersllc.com/blog/us-nationwide-data-privacy-law-gdpr/#:~:text=There%20is%20no%20federal%20data,held%20by%2US%20government%20agencies

Gartner (n.d.). Definition of Digitalization. https://www.gartner.com/it-glossary/digitalization/

General Agreement on Trade and Services (1995). *Article XIV: General Exceptions*. https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV

General Data Protection Regulation (2018). *European Union.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Gupta, S., & Ganguly, S. (2020, November 23). Why India Refused to Join the World's Biggest Trading Bloc. New Delhi chose protectionism over the RCEP. History suggests it made the wrong call. *Foreign Policy.* https://foreignpolicy.com/2020/11/23/why-india-refused-to-join-rcep-worlds-biggest-trading-bloc/

Herian, R. (2020, February). Blockchain, GDPR, and the fantasies of data sovereignty. *Law, Innovation and Technology, 12*(1), 156-174. https://doi.org/10.1080/17579961.2020.1727094

Hirsch, L., McCabe, D., Benner, K. & Thrush, G. (2022, September 26). TikTok Seen Moving Toward U.S. Security Deal, but Hurdles Remain. *New York Times.* https://www.nytimes.com/2022/09/26/technology/tiktok-national-security-china.html

Huang, R., & Shen, L. (2022, July 8). China introduces new rules governing cross-border transfers of data; many companies will have to seek approval before exporting data, increasing

compliance and business costs. *Wall Street Journal.* https://www.wsj.com/articles/china-introduces-new-rules-governing-cross-border-transfers-of-data-11657271646

Husch Blackwell (2022, July 18). *2022 State Privacy Law Tracker: A comprehensive resource for tracking U.S. state privacy legislation.* https://www.huschblackwell.com/2022-state-privacy-law-tracker

International Trade Administration. (2021, October 22). *India - Country Commercial Guide: Information and Communication Technology*. U.S. Department of Commerce. https://web.archive.org/web/20220727072457/https://www.trade.gov/country-commercial-guides/india-information-and-communication-technology

Kuner, C. (2015). Data nationalism and its discontents. *Emory Law Journal Online, 64*, 2089–2098. https://law.emory.edu/elj/elj-online/volume-64/responses/data-nationalism-its-discontents.html

Kurbalija, J. (2016). *An Introduction to Internet Governance* (7th ed.). DiploFoundation. https://www.diplomacy.edu/wp-content/uploads/2021/12/AnIntroductiontoIG_7th-edition.pdf

Lawfare. *Snowden Revelations.* https://www.lawfareblog.com/snowden-revelations

Magnuson-Moss Warranty - Federal Trade Commission Improvement Act (1975, January 4). Pub. L. No. 93-637, 88 Stat. 2183. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg2183.pdf.

Matthan, R., & Ramans, S. (2022, August). India's approach to data governance. In Feigenbaum, E.A. & Nelson, M.R. (Eds.), *Data Governance, Asian Alternatives: How India and Korea are creating new models and policies*, (pp. 11-32), Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/08/31/india-s-approach-to-data-governance-pub-87767

McBride, J., & Chatzky, A (2019, May 13). Is 'Made in China 2025' a Threat to Global Trade? *Council on Foreign Relations.* https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

McCabe, D. (2022, June 17). TikTok says its American traffic is going through Oracle servers, but it retains backups. *New York Times.* https://www.nytimes.com/2022/06/17/technology/tiktok-oracle-servers.html

National Conference of State Legislatures (2022, July 6). *State Laws Related to Digital Privacy*. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Office of the United States Trade Representative (2021, September 9). *Statement from Ambassador Katherine Tai on the Re-Launch of the U.S.-Mexico High-Level Economic Dialogue.* https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/september/statement-ambassador-katherine-tai-re-launch-us-mexico-high-level-economic-dialogue

Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines for Multinational Entreprises (2011 edition)*, https://www.oecd.org/daf/inv/mne/48004323.pdf

Park, K.S. (2022, August). Korea's path to best practices for cross-border data flows. In Feigenbaum, E.A., & Nelson, M.R. (Eds.), *Data Governance, Asian Alternatives: How India and Korea are creating new models and policies*, (pp. 11-32), Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/08/31/korea-s-path-to-best-practices-for-cross-border-data-flows-pub-87770

Parsheera, S. (2022, August). What's Shaping India's Policy on Cross-Border Data Flows? In Feigenbaum, E.A., & Nelson, M.R. (Eds.), *Data Governance, Asian Alternatives: How India and Korea are creating new models and policies*, (pp. 11-32), Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/08/31/what-s-shaping-india-s-policy-on-cross-border-data-flows-pub-87769

Potluri, S., Sridhar, V., & Rao, S. (2020. August 9). Effects of data localization on digital trade: An agent-based modeling approach. *Telecommunications Policy 44*(9). https://doi.org/10.1016/j.telpol.2020.102022

Regional Comprehensive Economic Partnership Agreement (2022, January 1). *RCEP Secretariat*. https://rcepsec.org/legal-text/

Regional Comprehensive Economic Partnership Agreement (2022, January 1). *RCEP Secretariat*. Chapter 12: Electronic Commerce. https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf

Rodriguez, S., & Palmer, D. (2020, September 14). IBM's new mantra: Resist 'data sovereignty'. *Politico*. https://www.politico.com/newsletters/weekly-trade/2020/09/14/ibms-new-mantra-resist-data-sovereignty-790378

Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. *The International Spectator*, *53*(4), 95-111. https://doi.org/10.1080/03932729.2018.1532705

Sampasa-Kanyinga, H., & Lewis, R. (2015). Frequent Use of Social Networking Sites Is Associated with Poor Psychological Functioning Among Children and Adolescents. *Cyberpsychology, behavior and social networking, 18,* 380-385. 10.1089/cyber.2015.0055

Schott, J. J. (2022, January 3). Which countries are in the CPTPP and RCEP trade agreements and which want in? *Peterson Institute of International Economics (PIIE)*. https://www.piie.com/research/piie-charts/which-countries-are-cptpp-and-rcep-trade-agreements-and-which-want

Sherman, J. (2019, October 30). How Much Cyber Sovereignty is Too Much Cyber Sovereignty? *Council on Foreign Relations.* https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

The Economist (2017, May 6). *The world's most valuable resource is no longer oil, but data.* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. (2018). Increases in depressive symptoms, suicide-related outcomes, and suicide rates among U.S. adolescents after 2010 and links to increased new media screen time. *Clinical Psychological Science*, *6*, 3–17. doi:10.1177/2167702617723376

United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996), June 12, 1996, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

United Nations Conference on Trade and Development (UNCTAD) (2021). *Digital Economy Report 2021 - Cross-border data flows and development: for whom the data flow.* https://unctad.org/system/files/official-document/der2021_en.pdf

United States Mexico Canada (USMCA) Agreement. July 1, 2020. https://www.trade.gov/usmca

U.S.-China Economic and Security Review Commission. (2022, July 26). *China's Evolving Data Governance Regime.* https://www.uscc.gov/sites/default/files/2022-07/Chinas_Evolving_Data_Governance_Regime.pdf

Utah Consumer Privacy Act (2022). S.B. 227. Effective December 31, 2023. https://le.utah.gov/~2022/bills/static/SB0227.html

Vila Seoane, M. F. (2021, May). Data securitisation: the challenges of data sovereignty in India. *Third World Quarterly, 42*(8), 1733-1750. https://doi.org/10.1080/01436597.2021.1915122

Virginia Consumer Data Protection Act (2021). Personal data rights of consumer, etc., HB 2307. https://lis.virginia.gov/cgi-bin/legp604.exe?ses=212&typ=bil&val=Hb2307

Virginia Consumer Data Protection Act (2021). Personal data rights of consumer, etc., SB 1392. Effective January 1, 2023. https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+SB1392

Walters, K. (2022). Reassessing the Mythology of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC. *Harvard Law & Policy Review, 16*. http://dx.doi.org/10.2139/ssrn.3875970

Wang, E. & Shepardson, D. (2022, March 10). EXCLUSIVE TikTok nears Oracle deal in bid to allay U.S. data concerns - sources. *Reuters*. https://www.reuters.com/technology/exclusive-tiktok-nears-deal-with-oracle-store-its-data-sources-2022-03-10/

Whitman, J. Q. (2004, April). The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal, 113*(6). https://www.yalelawjournal.org/article/the-two-Western-cultures-of-privacy-dignity-versus-liberty

White House. (2022, January 21). *Readout of President Biden's Meeting with Prime Minister Kishida of Japan.* https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/21/readout-of-president-bidens-meeting-with-prime-minister-kishida-of-japan/

White House. (2022, March 25). *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework.* 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. (2022, October 7). *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

World Trade Organization (2019, January 25). *DG Azevêdo meets ministers in Davos: discussions focus on reform; progress on e-commerce*. https://www.wto.org/english/news_e/news19_e/dgra_25jan19_e.htm

World Trade Organization. (n.d.). *Joint Initiative on E-commerce.* https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm

Wu, E. (2021, July). *Sovereignty and Data Localization.* The Cyber Project, Harvard Kennedy School Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf

Yasir, S. and Deep Singh, K. (2022, August 4). India withdraws a proposed law on data protection. *New York Times.* https://www.nytimes.com/2022/08/04/business/india-data-privacy.html

Zhu, J. (2022, February 14). The Personal Information Protection Law: China's Version of the GDPR? *Columbia Journal of Transnational Law.* https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr