Atlantic Council
GEOECONOMICS CENTER

ISSUE BRIEF

Competing Data-Governance Models Threaten the Free Flow of Information and Hamper World Trade

NOVEMBER 2021

HUNG TRAN

Essential ingredients of a globalized economy with integrated supply chains are the free movement of goods, services, capital, and data across national borders. As backlashes against globalization persist and geopolitical competition escalates, more and more barriers have been erected by many governments, making world trade more costly and less efficient. These measures include tariffs and other controls of trade flows, heightened screening of investment flows, and tightened immigration policies. The barriers are spreading to the realm of data flows, which are increasingly important in society and the economy. In 2019, for example, global digital trade, including e-commerce and digitally delivered services, was valued at $5.5 to $6 trillion, about 25 percent of total world exports.[1] "The world's most valuable resource is no longer oil, but data," declared The Economist in 2017.[2]

Consequently, debates are growing among citizens, businesses, and policymakers about the need for a governance framework for data, and for such frameworks to be coordinated internationally if possible. Indeed, the Third United Nations World Data Forum (October 3-6, 2021, in Bern, Switzerland) has emphasized the indispensable role of data and sharing data in solving problems facing the world, and advocated ways of enhancing trust in data by protecting data security and privacy, helping to preserve the free flow of information.[3]

1 Ingo Borchert et al., *G7 Leaders Should Discuss International Trade (Seriously),* UK Trade Policy Observatory, Briefing Paper 59, June 2021, https://blogs.sussex.ac.uk/uktpo/files/2021/06/BP59.pdf.

2 "The World's Most Valuable Resource Is No Longer Oil, But Data," *The Economist*, May 6, 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

3 International Institute of Sustainable Development, UN World Data Forum 2021, Earth Negotiations Bulletin (IISD reporting unit), October 3, 2021, https://enb.iisd.org/un-world-data-forum-2021-3Oct2021.

There are several dimensions of a data-governance framework. One looks at the stages in the data supply chain: the generation of data (including posting personal data online and consummating transactions online, which become data points), their collection, management (including quality control), usage (including marketing, research, political, and military), and transfer (both domestically and cross-border). Another dimension refers to the actors in the data ecosystem: Who owns the personal data? Who benefits from data? Who decides what to collect and how to use data points? Who controls them? Furthermore, the digital platforms that allow data to be exchanged and collected also need to be looked at, mainly due to the oligopolistic character of huge platform operators who can reap the benefits of network effects and incumbency—not only in terms of profits but also in terms of social and political influences.

Three different data-governance approaches have emerged. The European Union (EU) has put forward a fairly comprehensive framework to regulate various aspects of generating and using personal data—emphasizing the protection of personal data security and privacy. By contrast, China has recently promulgated a series of laws, formalizing its vision of data sovereignty (also referred to as digital or cyber sovereignty) and claiming that personal data concerning its citizens are under the authority of the government to safeguard economic development, social stability, and national security.[4] The United States has always insisted on the free flow of information and data, both domestically and internationally. It also focuses on protecting personal privacy against the government—except in cases of national security concerns. However, there is no federal law comprehensively protecting personal privacy vis-a-vis private-sector companies, especially on the Internet—except in specific areas such as personal health information.

As these regional/national data-governance frameworks are being formalized into laws, in many cases with extraterritorial overreach, the global marketplace for ideas, information, and data will be fragmented, raising the costs of compliance in doing cross-border business as well as limiting the potential to share data widely, which, among other things, has been crucial for fostering collaborative scientific research leading to innovation.

THE EU APPROACH

The EU has developed a comprehensive framework to regulate various aspects of data—including a person's rights to his or her data being collected, used, and transferred; noncompetitive behaviors of data intermediaries and platform companies; these entities' responsibilities for the content of their online services; as well as the taxation of their activities in an EU country even when the entities are headquartered in a third country.

Built on EU Privacy Directives, the General Data Protection Regulation (GDPR) became effective on May 25, 2018. The GDPR seeks to protect the fundamental rights of citizens regarding their personal data.[5] Basically, data intermediaries have to obtain consent from a person before sending information to or collecting data about the person. A person also has the right to request to see the content of the person's data, to ask for the ways such data have been used, to request corrections to the data, and deletion of the data altogether. The GDPR has significant extraterritorial reach as it applies to all data intermediaries, no matter where headquartered, if the data involve persons living in the EU.

The GDPR also stipulates that data concerning an EU citizen can only be transferred to entities in a non-EU country if that country is deemed by the European Commission to have a privacy protection regime functionally equivalent to that of the EU. This has led to a serious rupture in US-EU commercial relations: in July 2020, the Court of Justice of the EU (CJEU) ruled that the United States doesn't have a functionally equivalent protection regime as the EU—basically on the issues of the "government access to personal data for national security purposes and the rights of EU citizens in the United States to judicial review and redress."[6] It has therefore invalidated the European Commission's finding of US equivalency which underpins the EU-US Data Privacy Shield designed to facilitate free data flows between the two jurisdictions. As a consequence, a transatlantic data-transfer relationship valued at is being jeopardized, with businesses in both jurisdictions facing huge uncertainty—and therefore demanding a timely resolution.[7] Otherwise, if the dispute persists, it will make data localization a de facto condition for international companies doing online business in

4 Bertrand de La Chapelle and Lorrayne Porciuncula, *We Need to Talk about Data: Framing the Debate around the Free Flow of Data and Data Sovereignty*, Internet & Jurisdiction Policy Network, March 31, 2021, https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf.

5 "What is GDPR, the EU's New Data Protection Law?," GDPR EU, https://gdpr.eu/what-is-gdpr/.

6 Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of the GDPR on Data Flows and National Security*, Brookings Institution, August 5, 2020, https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.

7 U.S. Chamber of Commerce, "Transatlantic Data Flows: Moving Data with Confidence," September 20, 2021, https://www.uschamber.com/technology/data-privacy/transatlantic-dataflows.

European Commissioner for Values and Transparency Vera Jourova and European Commissioner for Justice Didier Reynders (R) give a news conference on EU rules on data protection (GDPR) and the new EU Strategy on victims' rights, in Brussels, Belgium, June 24, 2020. Source: Olivier Hoslet/Pool via REUTERS

and with the EU: it may be simpler to build data servers and processing facilities within the EU than deal with the legal uncertainty. Efforts to resolve this dispute are ongoing, with no clear prospects of conclusion anytime soon.

While the European Commission has recognized thirteen countries and territories as having adequate data-privacy protection, it is important to note that the CJEU ruling on the US regulatory framework could raise doubts about whether many of the other twelve countries, least of all China, could be deemed equivalent without being challenged by the CJEU.[8] If this uncertainty persists, the CJEU stance on foreign equivalency, as manifested in the case of the United States, risks restricting the flow of data from and to the EU, with possible negative implications for online businesses as well as for innovation, especially in data-intensive industries such as artificial intelligence (AI).

The CJEU has significantly strengthened the enforcement of the GDPR by allowing national privacy commissions (of member states) to take offending data companies to court, instead of having to rely on the EU lead privacy protection authority to file injunctions against cross-border data complaints.[9] However, this risks increasing national divergences in the interpretation and application of the GDPR, making compliance more difficult across the member states.

The Digital Markets Act (DMA) was proposed by the European Commission in December 2020 and currently is moving through the EU legislative process involving the European Parliament and member states.[10] The DMA aims to address the concentration of market power by big digital companies (so-called gatekeepers), essentially requiring them to grant access to their platforms to other businesses in certain situations; and to stop exclusionary and unfair practices vis-a-vis business users and customers to gain undue advantages. This initiative is expected to lead to more competition and a level playing field in the digital services market.

8 "Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

9 "EU Court Allows Data Protection Authorities to Sue Big Tech Companies," *Statecraft*, June 16, 2021, https://www.statecraft.co.in/article/eu-court-allows-data-protection-authorities-to-sue-big-tech-companies.

10 "The Digital Markets Act: Ensuring Fair and Open Digital Markets," European Commission, accessed November 2, 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

The Digital Services Act (DSA), launched at the same time as the DMA, is also going through the same legislative process. The DSA aims to improve the mechanism to ensure online-platform users' fundamental rights, including freedom of speech and the removal of illegal content. It is intended to strengthen public oversight of these platforms, especially the big ones reaching more than 10 percent of the EU population. In particular, citizens and watchdog organizations—including independent entities known as trusted flaggers that would theoretically be approved by (national) digital services coordinators—would help identify and alert the online platform operators to misinformation or other illegal content, which they would have to address including by removing that content according to a transparent and user-friendly procedure, which has not yet been established.[11]

Last but not least, a digital services tax (DST) was in place or proposed in eleven EU member countries (as of March 2021), and others inside and outside the EU were considering the approach.[12] Essentially, the DST is for multinational digital services companies whose global revenues exceed a certain threshold and in-country revenues exceed a lower threshold. For example, the United Kingdom's DST applies a 2 percent tax on the revenues of search engines, social media platforms, and online market places—but only on those whose global digital services revenues surpass £500 million ($674.5 million) and digital services revenues within the UK surpass £25 million.[13] The DST is being justified as a way to deal with the problem of tax evasion by multinational companies establishing their offices in low tax jurisdictions. This measure is, however, controversial, especially from the US perspective, as it deviates from the traditional concept of tax bases being the physical locations of companies' offices, not the location of the users, as well as being discriminatory against US-owned, multinational tech behemoths. The United States has threatened retaliatory measures against countries unilaterally implementing the DST, but some approved measures have been held in abeyance pending the outcomes of the Organisation for Economic Co-operation and Development (OECD) corporate-taxation negotiations.

The DST is a key part of the OECD-sponsored 130-country negotiations to reform the framework for international corporate tax reform—the other issue being agreeing to a minimum corporate income tax rate.[14] The OECD talks are expected to conclude soon, having just reached an agreement on a 15 percent minimum corporate income tax—which was endorsed by the Group of Twenty Summit in Rome on October 30-31, 2021. As part of the compromise, France, Austria, Italy, Spain, and the UK agreed to withdraw their DST measures in 2023 when the agreed global corporate tax regime takes effect; and the United States will drop its retaliatory punitive tariffs.[15]

While at different stages of enactment and implementation, the various components described above give the EU a comprehensive legal and regulatory framework to deal with the whole nexus of data and digital services. Basically, the thrust of the EU approach is to protect individuals against both corporate and government intrusion into, and possible abuse of, their personal data; trying to maintain a competitive environment for digital companies; and holding them responsible for dealing with complaints about the content of the data transmitted over their networks.

THE CHINESE APPROACH

The Chinese approach can be gleaned from a series of recently passed laws, together with the statements and actions of the Communist Party of China (CPC) and government leaders. The basic law is the 2017 Cybersecurity Law, which articulates the concept of data sovereignty, and details the obligations of Internet products and services providers and operators in data gathering, localization (with servers located in China), usage, and transmission, especially overseas—all in the interest of national security.[16] The law also specifies that Internet operators have to cooperate and turn over user data to public and national security organs when requested: this reinforces a key article of the National Intelligence Law of 2017.[17] The companies also

11 "European Commission Plan to Reform Europe's Digital Space–Part 2–Drafting Digital Service Act," O'Melveny & Myers LLP , December 23, 2020, https://www.omm.com/resources/alerts-and-publications/alerts/european-commission-plan-to-reform-europes-digital-space-part-2/.

12 Elke Asen, "What European OECD Countries Are Doing About Digital Service Taxes," Tax Foundation, March 25, 2021, https://taxfoundation.org/digital-tax-europe-2020/.

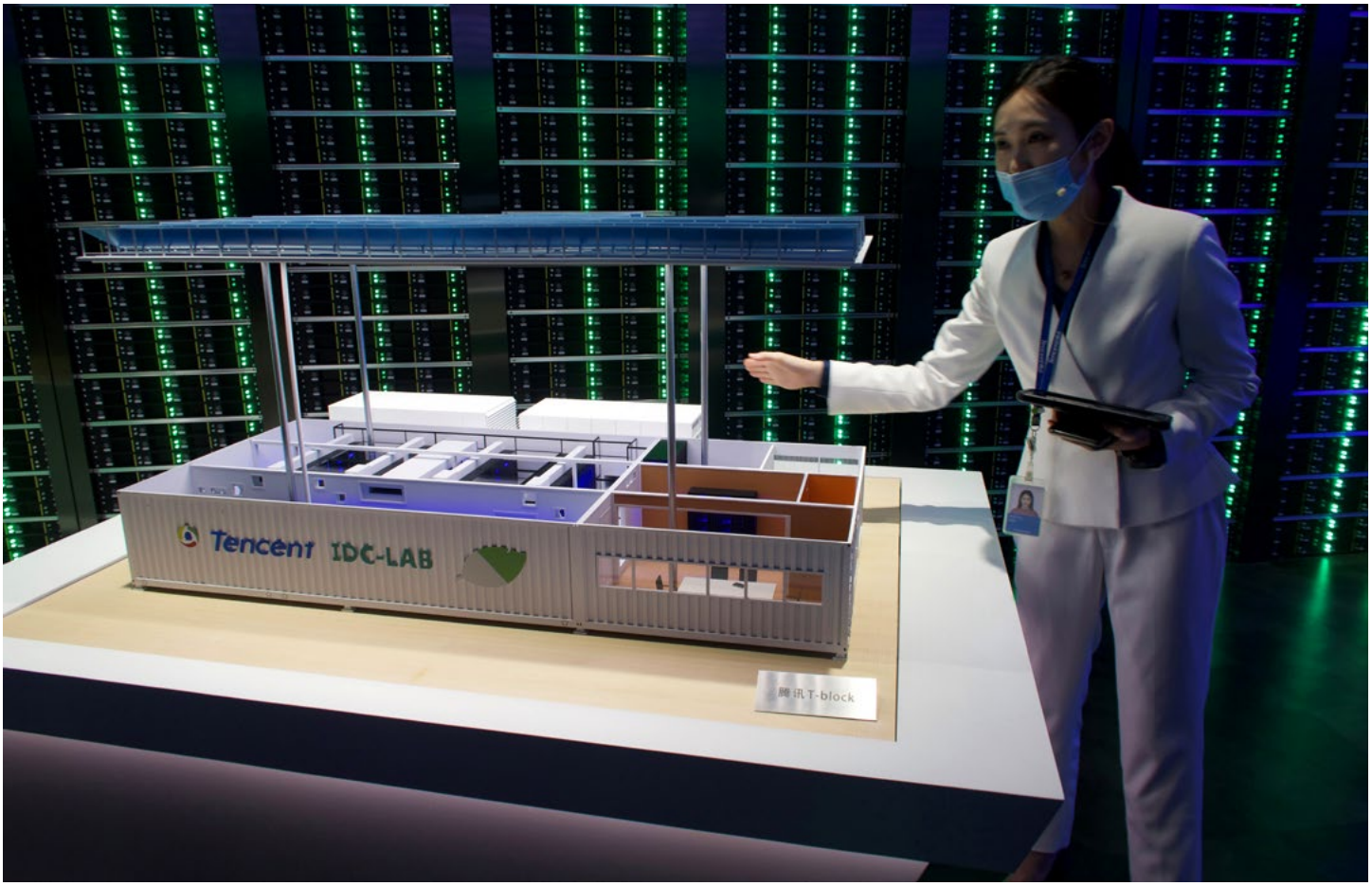
13 Office of the United States Trade Representative, *Section 301 Investigation: Report on the United Kingdom's Digital Service Tax*, January 13, 2021, 6, https://ustr.gov/sites/default/files/files/Press/Releases/UKDSTSection301Report.pdf.

14 "130 Countries and Jurisdictions Join Bold New Framework for International Tax Reform," OECD, July 1, 2021, https://www.oecd.org/newsroom/130-countries-and-jurisdictions-join-bold-new-framework-for-international-tax-reform.htm.

15 "US Reaches Agreement to End European Digital Services Taxes," *Deutsche Welle* (DW), October 22, 2021, https://p.dw.com/p/420jb.

16 Jack Wagner, "China's Cybersecurity Law: What You Need to Know," *The Diplomat*, June 02, 2017, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

17 Murray Scot Tanner, "Beijing's New International Intelligence Law: From Defense to Offense," *Lawfare* (blog), Lawfare Institute in Cooperation with the Brookings Institution, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.



A staff member introduces Tencent's Internet Data Center (IDC) cloud computing service during a government-organized media tour to Tencent headquarters in Shenzhen, Guangdong province China September 27, 2020. Picture taken September 27, 2020.
Source: REUTERS/David Kirton

are responsible for the content transmitted over their networks. The privacy of individual users is mentioned.

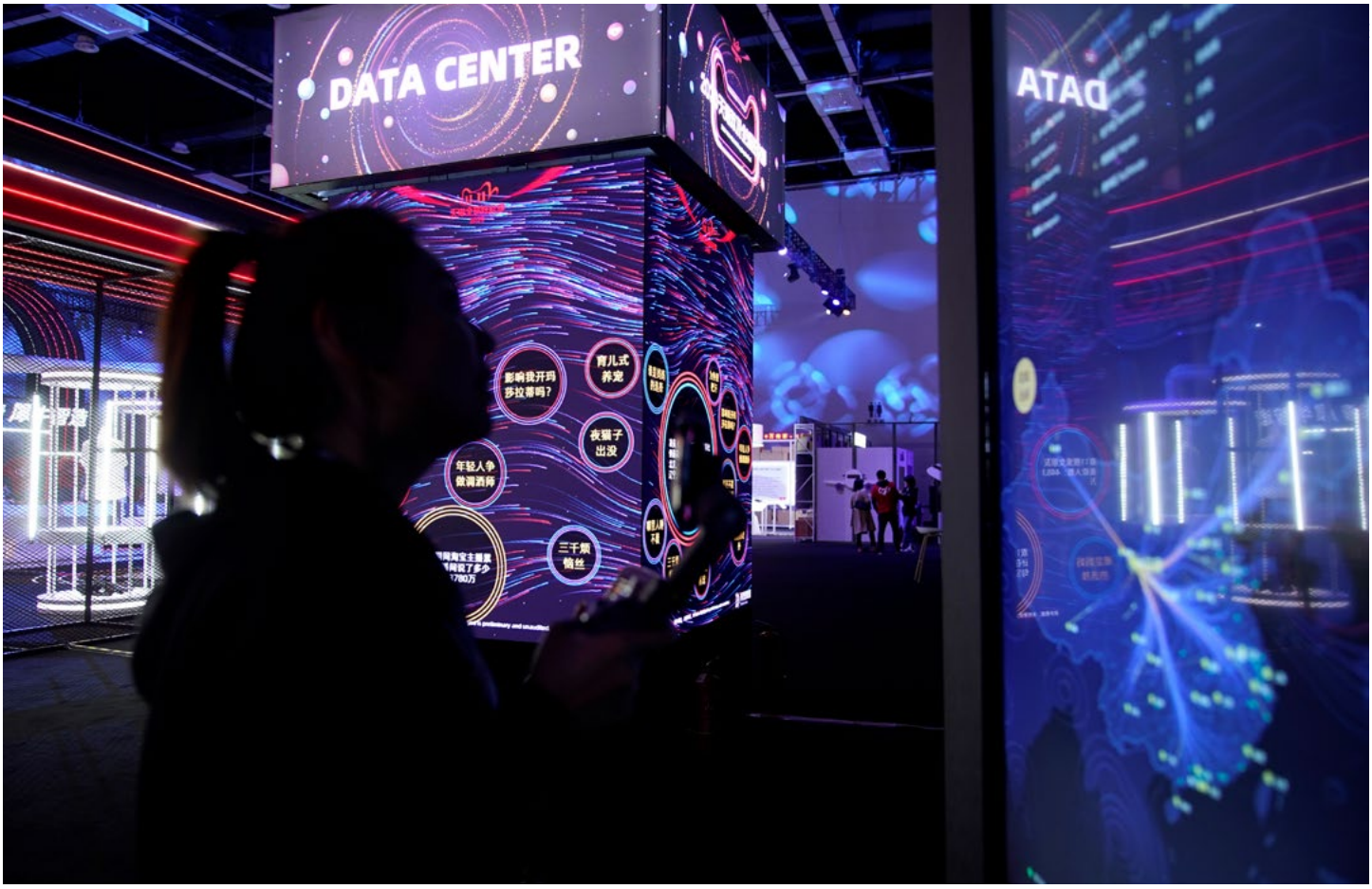
Next is the Data Security Law (passed in September 2021), which tightens restrictions on data transfer outside of China and imposes wide-ranging data security obligations on companies.[18] In particular, the law appends a new "national core data" category which includes data affecting national security, the domestic economy, people's livelihoods, and the public interest at large. Such a vague definition allows ample room for government officials to interpret and implement the law, increasing uncertainty for companies.

Complementing those laws are the Personal Information Protection Laws (PIPL), effective November 1, 2021.[19] The PIPL applies to personal information processing entities (PIPEs), imposing strict requirements on cross-border transmission of personal information, including informing the persons, obtaining their consent, and ensuring that data recipients, including those outside China, satisfy the standards of PIPL—meaning the law applies extraterritorially. The law gives the Chinese government broad authority in processing personal information. However, the PIPL also defines the legal rights of persons vis-a-vis companies, which have to obtain consent, and to provide ways for such consent to be withdrawn, before collecting personal information. As a result, the PIPL shares some similarities with the GDPR in this respect.

Basically, China's aim is to regulate the use of data to protect its national security, not only with regard to the outward transfers of data but also inward dissemination of information (by erecting what's been dubbed the Great Firewall to exclude what Beijing regards as undesirable information from coming in). China has also built out the hardware (such as ubiquitous cameras in public spaces that are enhanced with facial recognition algorithms) and systems (such as its social credit scoring system, which is in development) to more effectively use data to monitor and control its population, including censorship

18 National Law Review, "China Passes New Data Privacy and Security Laws," *The National Law Review*, August 23, 2021, https://www.natlawreview.com/article/china-passes-new-data-privacy-and-security-laws.

19 "China Passes the Personal Information Protection Law to Take Effect on November 1," Gibson Dunn, September 10, 2021.



A woman checks data of Alibaba Group's Singles' Day global shopping festival at a media center in Hangzhou, Zhejiang province, China November 11, 2020. Source: REUTERS/Aly Song

of information and suppression of online activities deemed undesirable by the government. As a result, many observers have referred to China's data sovereignty as data or digital authoritarianism. These laws were recently used to rein in major Chinese platforms, social media, and transportation companies by Chinese authorities for what is deemed oligopolistic behaviors or failure to establish adequate safeguards against unauthorized transfers of data to foreign entities.

China has been active in pushing for recognition of key features of its data sovereignty vision in setting international technological standards. For example, at the International Telecommunications Union (ITU), China has proposed New Internet Protocols enabling government control of developments and activities on the Internet, to replace the current global, open, and decentralized protocols.[20] Moreover, China has been able to export its concept of data sovereignty and enabling hardware and systems to other countries, mainly but not exclusively in Asia and Africa.[21]

However, it is important to note that China is not the only inspirational source of data sovereignty. India, a populous democratic country, opposes China on many fronts, but has adopted almost the same approach as China, with the exception of practices such as censorship of online information. India claims data sovereignty and uses social stability, human rights, national security, and the need to fight "data colonialism" of Western companies as justifications to control personal data, including requiring data localization.[22] Indeed, India has banned fifty-nine Chinese Internet apps including TikTok, WeChat, and an Alibaba unit's UC Browser because they were "prejudicial to [the] sovereignty and integrity of India, defense

20 Madhumita Murgia and Anna Gross, "Inside China's Controversial Mission to Reinvent the Internet," Financial Times, March 27, 2020, https://on.ft.com/3eMzGoJ.

21 Mathew S. Erie and Thomas Streinz, *Understanding China's Growing Influence in Global Data Governance*, US-Asia Law Institute, April 1, 2021, https://usali.org/usali-perspectives-blog/understanding-chinas-growing-influence-in-global-data-governance.

22 Susan Ariel Aaronson, *Data is Disruptive: How Data Sovereignty Is Challenging Data Governance*, Hinrich Foundation, August 2021, https://research.hinrichfoundation.com/hubfs/White%20Paper%20PDFs/How%20data%20sovereignty%20is%20challenging%20data%20governance%20(Susan%20A.%20Aaronson)/Data%20is%20disruptive%20-%20Hinrich%20Foundation%20white%20paper%20-%20Susan%20Aaronson%20-%20August%202021.pdf?__hsfp=113833972&__hssc=251652889.46.1633422472083&__hstc=251652889.54c0a874246e53cd709fc884517b5784.1632828376093.1632828376093.1632828376093.1.

of India, security of state, and public order."[23] Specifically, the Information Technology Act (of 2011) and other rules regulate the collection and disclosure of personal data to safeguard data security and privacy—but the government is not subject to those rules (like in China).

THE US APPROACH

The United States does not have a comprehensive federal law for data protection similar to the GDPR. Instead, it has a collection of specific federal laws and some state consumer privacy laws. The main law aims to protect personal data from the government, not private-sector companies. The US Privacy Act of 1974 prescribed restrictions on the use of personal data held by government agencies and affirmed the right of citizens to access, copy, and correct their data held by the government. However, the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act of 2018) "allows US law enforcement agencies to issue warrants to gain access to data held by organizations under US jurisdiction, even if such data is held outside the US and such data involves individuals other than US citizens."[24]

Specific laws have been passed to protect the security and privacy of specific types of personal data. For example, the Health Insurance Portability and Accountability Act (1996) institutes national standards for the protection of certain health information, including that being stored or transferred electronically.[25] Furthermore, it sets confidentiality requirements for the use and sharing of protected health information (PHI). The Children Online Privacy Protection Act (2000) prohibits online companies from collecting personal information from minors—especially those below twelve years of age, unless there is verifiable parental consent.[26] The landmark financial-sector reform act, the Gramm-Leach-Bliley Act (1999), contains sections protecting nonpublic personal information arising from financial transactions with services providers.

More importantly, there is no comprehensive federal law concerning data privacy on the Internet similar to the GDPR. In that vacuum, several US states have proposed legislation

Sheila Colclasure, global chief digital responsibility and public policy officer at IPG Kinesso, and Charlotte Slaiman, competition policy director at Public Knowledge, swear in during Senate Judiciary Competition Policy, Antitrust, and Consumer Rights Subcommittee hearing on "Big Data, Big Questions: Implications for Competition and Consumers" in Washington, D.C., U.S., September 21, 2021. Source: Ting Shen/Pool via REUTERS

to protect consumer data privacy.[27] As of this writing, the California Consumer Privacy Act became effective on January 1, 2021; the Virginia Consumer Data Protection Act has a delayed effective date in 2023; and six other states have bills in the works. Basically, these state laws share some similarities with the GDPR in affirming a person's rights of access, rectification, and deletion of the personal data collected by companies that have to meet their obligations in data usage.

SUMMING UP—KEY DIFFERENCES

Broadly speaking, the key difference is between the EU and Chinese models, with the US model landing somewhere in between but closer to the EU framework. The EU model emphasizes citizen rights to personal data privacy, offering protection from both private companies and governments. This model aims to regulate the concentration of market power by big platform companies; holds them responsible for content in

23 "India Permanently Bans Tiktok and 58 Other Chinese Apps," *Nikkei Asia*, January 26, 2021, https://asia.nikkei.com/Business/Technology/India-permanently-bans-TikTok-and-58-other-Chinese-apps.

24 Matthias Artzt and Walter Delacruz, "How to Comply with Both GDPR and the CLOUD Act," International Association of Privacy Professionals, January 29, 2019, https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/.

25 U.S. Department of Health and Human Services, "Summary of the HIPPA Security Rule," accessed November 2, 2021, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

26 Federal Trade Commission, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business," accessed November 2, 2021, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

27 International Association of Privacy Professionals, "US State Privacy Legislation Tracker," last updated May 26, 2021, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law.pdf.

general, including in particular misinformation and malicious activities; and sets out to tax multinational platform companies for activities in their jurisdictions. One particular component of the European framework—the GDPR—has attracted much international compliance by non-EU companies doing business with EU residents (a manifestation of the "Brussels effect"); and it has been used by many countries as a template to develop their own data-privacy laws (so far sixteen countries have enacted national legislation modeled on the GDPR.) [28]

By contrast, the Chinese model focuses on defending China's sovereignty and security, giving broad authority to the government to access and process data collected by companies, which are required to protect the security and privacy of the data vis-a-vis other companies. It also strictly controls the transfer of data to entities outside of China (including via data localization) as well as inward transfer of data to China (especially information deemed undesirable, using the Great Fire Wall). China has developed a high-tech infrastructure to implement the data control regime. Many countries, especially in the developing world, have adopted features of China's model, in particular asserting their data sovereignty and importing the hardware and software to implement it.

US federal laws aim to protect citizen privacy against the government but not against private companies, except in the case of health and financial information and data on children. The US Congress is currently considering antitrust measures against big platform and social media companies; strengthening online privacy protection for minors; and more generally, narrowing or repealing Section 230 of the Communication Decency Act (1996), which has protected social media companies from being held liable for the content of users' posts.[29] Moreover, several states have taken initiatives to propose and pass data-privacy protection laws regarding companies along the lines of the GDPR. If more and more US states move in this direction, the federal government may feel it necessary to take actions to ensure uniformity across states. The federal nature of the US political system makes it difficult for other countries to adopt its mixed data-governance model.

DATA GOVERNANCE AND TRADE AGREEMENTS

Among the three major data-governance models and their variations, the main fault line is between the free flow of data across borders versus requirements of data localization and government access to companies' algorithm and source code. The United States has been the main driving force in insisting on the unconstrained flow of data and banning data localization and government access to algorithm and source code in trade talks—in particular during the Trans Pacific Partnership (TPP) negotiations. After the US withdrawal, the remaining TPP partners finished the deal under the name Comprehensive and Progressive Trans Pacific Partnership (CPTPP), and retained much of the free flow of data provisions. The Trump administration then negotiated tougher language promoting the free flow of data in the US-Mexico-Canada Agreement (USMCA), the US-Japan Digital Trade Agreement, and US-South Korea trade deal. A few recent deals such as the Digital Economy Agreement (DEA) between Australia and Singapore moved further by agreeing to collaborate on data standards and regulatory coherence, promoting interoperable data-governance rules among the signatories.

However, most of those trade agreements include exceptions to the ban on data localization and sharing of algorithm and source code with the government, when justified by public policy. In many agreements, the exception has been worded very broadly and loosely, basically allowing member countries to invoke privacy protection, social stability, or national security to require data localization. In particular, the Regional and Comprehensive Economic Partnership (RCEP) permits member countries to make use of the exceptions without being challenged by other signatories. Basically, the fact that a country like China, with clear data-localization requirements and other restrictions, is a founding member of RCEP suggests that its provision against data localization is meaningless.

At present, it appears that more and more countries are moving toward data-localization requirements, either de jure as parts of their claims of data sovereignty or de facto

28 Mike Woodard, "16 Countries with GDPR-like Data Privacy Laws," Security Scorecard (company website), July 8, 2021, https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws.

29 Marcy Gordon, "After the Facebook Papers, How Will Congress Regular Social Media?," Associated Press story in Christian Science Monitor, November 1, 2021, https://www.csmonitor.com/Technology/2021/1101/After-Facebook-Papers-how-will-Congress-regulate-social-media.

when they insist that data can only be transferred freely to countries deemed to have adequate privacy protection. In fact, the number of countries having enacted data-localization legislation has increased from thirty-five in 2017 to sixty-four in 2021.[30] The tendency of many countries to require data localization is becoming a difficult obstacle to making progress in negotiating digital trade deals. For example, since 2019 the World Trade Organization (WTO) has tried to negotiate rules covering cross-border data flows in a plurilateral (as opposed to multilateral) effort involving eighty-six members, with seventy-eight developing countries refusing to participate.[31] The WTO negotiations have finalized texts on spam, electronic signatures, and authorization. However, the sticking points remain the language governing cross-border data flows and rules covering new services based on data such as AI.

Data-localization requirements act as nontariff barriers to digital services trade and promote an unlevel playing field favoring domestic companies at the expense of foreign ones. Consequently, these requirements will reduce the efficiency of digital data trade and the chance of using trade agreements to seek internationally agreed rules on cross-border data flows.

Even the United States and the EU, which share many democratic values, continue to differ on several data-governance issues, making a complete alignment between the two difficult. These issues include how to police the content of online information; the liabilities of platform companies regarding content; data localization; the US demand to have access to personal data on national security grounds; and the subject of digital services taxation. The joint statement issued on September 29, 2021, after the inaugural meeting of the EU-US Technology and Trade Council mentioned (among the meeting's outcomes) tasking the Data Governance and Platform Governance Working Group with exchanging information on respective approaches, "seeking consistency and interoperability where feasible"—meaning the differences on data governance between the two remain.[32]

CONCLUSION

Overall, there is a clear opposition between China's model of data sovereignty/authoritarianism (which is being followed by a growing number of developing countries) and the Western model focusing on protecting personal rights to data security and privacy. The latter has been typified by the EU approach, in particular its GDPR, which many countries have used as a template for their own legislation, albeit with some variations. Beyond the fundamental fault line between these two systems, data-localization requirements—de jure or de facto—have spread more widely despite support from the United States and others for the free flow of data. These requirements will have serious implications for the world economy. First of all, the different legal and regulatory regimes will serve as nontariff barriers to trade—not only in data services but eventually in telecom and computing hardware and software, including for cloud services, which are critical backbones for the flow of data. Secondly, they will restrict the free flow of data and information, which has contributed significantly to the functioning of the world economy, and in particular, fostered scientific and medical research collaboration and innovation that can spur growth. The global flow of data now contributes more to global growth than trade in goods, according to the US Chamber of Commerce.[33] Without the free flow of data, global trade would be hampered and growth potential weakened. More ominously, it would deepen the division of the world into competing systems.

Hung Q. Tran is a nonresident senior fellow at the Atlantic Council's Geoeconomics Center. Mr. Tran is an accomplished economist, with broad experience across the private sector, international organizations and research institutions. From 2007 till retirement in 2018, Mr. Tran was at the Institute of International Finance (IIF). Since 2012 he served as IIF's Executive Managing Director while simultaneously leading its Global Capital Markets Department. Prior to his work at the IIF, Mr. Tran served for six years at the International Monetary Fund as Deputy Director for the Monetary and Capital Markets Department. In the previous two decades, he was in senior positions managing economic and investment research at Rabobank, Deutsche Bank, Merrill Lynch and Salomon Brothers.

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

31 Aaronson, *Data is Disruptive*.

32 European Commission, *EU-US Trade and Technology Council Inaugural Joint Statement*, EU (Press Corner website), September 29, 2021, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951.

33 U.S. Chamber of Commerce, *Transatlantic Data Flows*.

ATLANTIC COUNCIL BOARD OF DIRECTORS

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org