Atlantic Council

EUROPE CENTER

ISSUE BRIEF

More than Adequate: New Directions in International Data Transfer Governance

JUNE 2023 Kenneth Propp

The **Europe Center** conducts research and uses real-time analysis to inform the actions and strategies of key transatlantic decisionmakers in the face of great power competition and a geopolitical rewiring of Europe. The Center convenes US and European leaders to promote dialogue and make the case for the US-EU partnership as a key asset for the United States and Europe alike.

The **Europe Center's Transatlantic Digital Marketplace Initiative** seeks to foster greater US-EU understanding and collaboration on digital policy matters and makes recommendations for building cooperation and ameliorating differences in this fast-growing area of the transatlantic economy.

Executive Summary

The US government and the European Union (EU) have made notable recent progress toward putting transatlantic data transfers on a more stable footing. They reached agreement on a new legal framework to replace the Privacy Shield,[1] and both signed on to an Organisation for Economic Co-operation and Development (OECD) Declaration on Government Access to Personal Data Held by Private Sector Entities.[2] Europe's distrust of commercial data flows to the United States—a concern ever since former National Security Agency contractor Edward Snowden's revelations a decade ago about their use as an avenue for US intelligence collection—seems to be less acute, as its attention to Russia and China increases.

But it would be a mistake for digital policy makers in Washington and Brussels now to put down their pens and declare the privacy problem solved. The new Data Privacy Framework (DPF) could well be found insufficient by the Court of Justice of the European Union. Even if the DPF survives, the United States and Europe risk drifting further apart in their pursuit of differing visions for the relationship between digital trade and privacy protections. The United States' inter-

1. US President Joe Biden and European Commission President Ursula von der Leyen announced the agreement in principle in March 2022. See: "United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework," White House, March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/#:~:text=Under%20the%20Trans-Atlantic%20Data%20Privacy%20Framework%2C%20the%20United,to%20ensure%20compliance%20with%20limitations%20on%20surveillance%20activities. On October 7, 2022, Biden signed an executive order establishing a Data Privacy Review Court to be located within the US Department of Justice. See: "Enhancing Safeguards for United States Signals Intelligence Activities," *Federal Register*, October 14, 2022, https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities. The European Commission responded on December 13, 2022, by proposing to find transfers to the United States made pursuant to the agreed Data Privacy Framework to be "adequate" for purposes of European Union (EU) law. See: "Adequacy decision for the EU-US Data Privacy Framework," European Commission, December 13, 2022, https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en.
2. "Declaration on Government Access to Personal Data Held by Private Sector Entities," OECD Legal Instruments, May 13, 2023, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

national posture is hampered by Congress' continued delay in adopting comprehensive national privacy legislation, making it a global outlier.

Many countries' privacy laws follow the model of the EU's General Data Protection Regulation, including its approach of conditioning unrestricted international data flows on the adequacy of foreign privacy protections. Not all countries necessarily reached the same conclusions about individual third countries' adequacy as the EU, however. In addition, the EU's own capacity to decide on third countries' adequacy is limited and cannot scale globally. The resulting complexity bogs down international data transfers in a web of repetitive documentation and legal uncertainty.[3] As the scale of global data flows multiplies, the need for broader interoperable mechanisms for international data transfer has only grown more acute.

This issue brief argues that there are a range of bilateral and multilateral initiatives that, over time, could bring greater policy coherence to transatlantic—and global—data transfers. Could a new US-EU bilateral accord on digital trade be salvaged from the abandoned Transatlantic Trade and Investment Partnership negotiations? Could the US-EU Trade and Technology Council play a role in developing common thinking on corporate and government accountability for personal data? Is there still hope for universal data transfer provisions to emerge from the long-running World Trade Organization e-commerce negotiations? Might multilateral organizations like the OECD or the Council of Europe (CoE) build on their successes in crafting international accords on privacy protection to defuse ever-present tensions about government surveillance? Is the Data Free Flow with Trust initiative championed by Japan a way to bridge regional differences? Might the newly expanded Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System achieve global relevance?

The multiplicity of efforts in international groupings to tackle the data transfer challenge may itself prove to be productive. Moving the discussion beyond the transatlantic frame offers the prospect of pragmatic multilateral solutions. There are even conceivable synergies among multilateral efforts, with linkages being explored among the work of the OECD, CoE, and Group of Seven, to mention a few. It is just possible that a more coherent global data transfer architecture is gradually emerging.

Introduction

Section 1 of this issue brief describes how central digital commerce has become to the transatlantic economy, galvanized by external shocks as diverse as the Russia-Ukraine war and the COVID-19 pandemic. Data transfers underlie much digital trade, but they are inherently susceptible to fears about national security services' exploitation for surveillance purposes. Section 2 then explains the varying US and European Union (EU) approaches to protecting privacy interests in data that is transferred internationally. The result, as Section 3 explains, is an increasingly tangled network of legal regimes that impose costs and uncertainty on international commerce.

Years of effort in Washington and Brussels to increase compatibility between privacy protections for personal data may finally be yielding a more sustainable transatlantic data transfer regime, Section 4 notes. But the system remains vulnerable to judicial challenge, so it behooves both governments to explore other bilateral directions as well. They could pursue a sector-specific digital trade agreement and utilize the US-EU Trade and Technology Council (TTC) to deepen shared understanding on data transfer risk assessment, as Section 5 explains.

There also is merit in looking systematically at multilateral settings where transatlantic differences are less magnified. Section 6 surveys fora for negotiating a more coherent multilateral dataflow regime, ranging from the World Trade Organization (WTO) to European and Asia-Pacific groupings.

1. The Geoeconomic and Geopolitical Importance of Transatlantic Data Transfers

The United States and the EU are each other's leading commercial partners in exporting and importing digitally enabled services. In 2020, such services accounted for nearly three-quarters of all US services exports, two-thirds of all services imports, and the vast majority of the US global surplus in trade in services. The picture is similar in the EU where digitally enabled exports and imports form a significant majority of the bloc's overall services trade with non-EU countries. The United States alone was the destination for nearly a quarter of the EU's such exports outside the bloc, and a third of its imports.[4]

3. OECD, "Moving forward on data free flow with trust: New evidence and analysis of business experiences," OECD Digital Economy Papers no. 353 (April 27, 2023), 15, https://doi.org/10.1787/1afab147-en.
4. Daniel S. Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2022* (Washington, DC: Foreign Policy Institute, Johns Hopkins SAIS/Transatlantic Leadership Network), ix.

TikTok CEO Shou Zi Chew testifies before a House Energy and Commerce Committee as lawmakers scrutinize TikTok's future in the United States, in Washington DC. March 23, 2023. REUTERS/Evelyn Hockstein

Measurements of global cross-border data flows also underscore the dominant transatlantic share. The largest shares of such flows are between Europe and North America, with the United States, the United Kingdom, Germany, and France comprising the four countries with the most. Much of the infrastructure for these transfers is supplied by subsea cables and data centers operated by US "hyperscalers."[5]

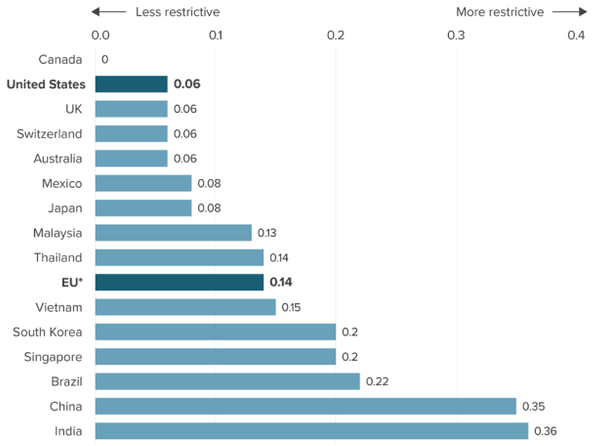
The war in Ukraine has driven home the importance of security of cloud services for the continuity of governments. As Russia launched information warfare against Ukraine's data systems, the Ukrainian government moved rapidly to shift from more vulnerable ones located at home to cloud-based hosting abroad. US cloud service providers have assisted the Ukrainian government in detecting and combatting cyberattacks.[6] Meanwhile, the advent of widespread remote work during the COVID-19 pandemic highlighted the economic importance of the digital economy.

Yet there are countervailing policy pressures to restrict cross-border data flows despite their economic and security value. Data "localization"—mandates that personal data generated within a jurisdiction be stored and processed there—has become politically attractive in many countries, which see it as a means of demonstrating digital sovereignty.[7] Governments may turn to localization because they suspect foreign intelligence services will intercept personal data in international transit or exploit it when it is stored or processed abroad.

Even the United States and EU, which in principle support cross-border data flows, have begun to consider and impose restrictions on transfers to certain countries. The European Data Protection Supervisor has sounded the alarm about China and Russia,[8] and the European Parliament has had a study of China's data protection regime undertaken.[9] US President Joe Biden Jr.'s administration and the US Congress are considering whether to impose limits on the ability of the social platform TikTok, owned by Chinese firm ByteDance, to transfer data from the United States to China.[10] Both Washington and Brussels have moved to block the use of TikTok by government employees.[11] There is even sentiment in some EU member states to restrict the use of US-based apps such as Insta-

5. Ibid., 57-59.
6. Cynthia Brumfield, "Russia-linked cyberattacks on Ukraine: A timeline," CSO, August 24, 2022, https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html.
7. Frances G. Burwell and Kenneth Propp, *Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy, Europe Center, Atlantic Council*, October 2022, 2, https://www.atlanticcouncil.org/wp-content/uploads/2022/11/Digital-sovereignty-in-practice-The-EUs-push-to-shape-the-new-global-economy_.pdf.
8. European Data Protection Supervisor, *Annual Report 2021*, November 8, 2021, https://edps.europa.eu/system/files/2022-04/2022-04-20-edps_annual_report_2021_en.pdf.
9. Paul de Hert and Vagelis Papakonstantinou, *The data protection regime in China*, 2015, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, European Parliament, https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf.
10. Elias Groll, "Inside TikTok's proposal to address US national security concerns," CyberScoop, January 27, 2023, https://cyberscoop.com/tiktok-national-security-cfius/?&web_view=true. The RESTRICT Act has been introduced in Congress to broadly empower the executive to ban TikTok's activities in the United States. See: RESTRICT Act, S. 686, 118th Cong. (2023-2024), https://www.congress.gov/bill/118th-congress/senate-bill/686/text?s=1&r=15.
11. Jamil Anderlini and Clothilde Goujard, "Brussels moves to ban Eurocrats from using TikTok," *Politico*, February 23, 2022, https://www.politico.eu/article/european-commission-to-staff-dont-use-tiktok/.

The US-EU divide in restrictiveness of digital services
Digital services trade restrictiveness index, 2022



Source: https://sgp.fas.org/crs/misc/IF12347.pdf • CRS/OECD
*EU27, excluding Bulgaria, Croatia, Cyprus, Malta, and Romania where no data were available

gram on the grounds that US national security agencies could exploit data transfers from Europe.[12]

2. Divergent US and EU Approaches to Privacy and Digital Trade

Countries regulate privacy according to their own constitutional traditions, yielding divergent approaches.[13] In the United States, the Supreme Court has recognized a right to privacy in cases arising principally in the criminal law and reproductive health areas, but the right does not appear explicitly in the US Constitution itself. Consumer protection law serves as the principal means for safeguarding Americans' interests in their personal information in the commercial setting.

Europe, by contrast, views the right to privacy—and its close cousin, the right to data protection[14]—as a matter, in the first instance, of fundamental rights enumerated in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights. The Court of Justice of the European Union (CJEU) case law permits interference with these rights only to the extent that it is necessary, proportionate, and not violative of the "essence" of the rights.[15] Other modern constitutions around the world also often contain an express right to privacy.

These differing visions of privacy as primarily a consumer right in the United States and a fundamental right in Europe carry over into the international trade setting. Several recent US free trade agreements (FTAs) contain sweeping guarantees of the ability to transfer data across transnational digital networks.[16] The Trans-Pacific Partnership (TPP) pursued by the Obama administration would have widened the circle to a large number of Pacific Rim countries, but the Trump administration abandoned the initiative and the Biden administration has not rejoined it.[17]

A number of Asian countries,[18] as well as some in Latin America, have adopted the US approach on data flows in their own FTAs. The EU's newest trade agreements also prohibit some specific types of restrictions on data transfers, for example, a number of those associated with localization, but tellingly lack a comparable overarching commitment to free data flows.[19]

Both US and EU FTAs recognize the right of governments to limit data transfers for regulatory reasons, including privacy protection. However, US agreements insist that restrictive regulatory measures be strictly necessary and not constitute arbitrary or unjustifiable discrimination nor disguised restrictions on trade in services between countries.[20] These constraints are derived from the exceptions allowed under the WTO's General Agreement on Trade in Services (GATS).[21]

Although the EU is a party to GATS, its subsequent bilateral trade agreements expressly allow each party to impose whatever limitations it deems appropriate for reasons of pri-

12. Laura Kayali, "It's not just TikTok: French also warn against WhatsApp, Instagram," *Politico*, March 22, 2023, https://www.politico.eu/article/french-top-officials-warn-lawmakers-against-using-tiktok-whatsapp-instagram/.
13. See, for example, James Q. Whitman, "'Human dignity' in Europe and the United States: the social foundations" in *European and US Constitutionalism*, ed. Georg Nolte (Cambridge University Press, 2009).
14. The Charter of Fundamental Rights of the European Union, a binding instrument of equivalent primary law value to the governing treaties of the EU, contains both a right to respect for private life (art. 7) and a right to the protection of personal data (art. 8). The latter has roots in the right of informational self-determination in Germany's Basic Law. "Charter of Fundamental Rights of the European Union," *Office of the Journal of the European Union*, October 26, 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.
15. Ibid., art. 52.
16. Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text, art. 19.11, Office of the United States Trade Representative, accessed May 13, 2023, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between. Agreement between the United States and Japan concerning digital trade, art. 11, Office of the United States Trade Representative, accessed May 13, 2023, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.
17. After the United States backed away from the Trans-Pacific Partnership in 2017, the other countries proceeded on their own with the agreement, rechristened the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP).
18. See, for example, Australia-Singapore Digital Economy Agreement, art. 23, Department of Foreign Affairs and Trade, Australian Government, accessed May 13, 2023, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement.
19. See, for example, Free Trade Agreement between the European Union and New Zealand, art. 12.4.2, accessed May 13, 2023, https://www.mfat.govt.nz/assets/Trade-agreements/EU-NZ-FTA/Text/Consolidated-Text-of-all-Chapters-including-the-Preamble.pdf.
20. Agreement between the United States of America, the United Mexican States, and Canada, art. 19.11.2.
21. General Agreement on Trade in Services, art. XIV bis, World Trade Organization, accessed May 13, 2023, https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm.

THE GLOBAL SCOPE OF ADEQUACY DECISIONS

Countries which utilize adequacy decisions on third-countries' data privacy standards to allow the free flow of personal data.

Source: International Association of Privacy Professionals

vacy or data protection.[22] The EU's firm insistence on such a "self-judging" privacy exception proved a major obstacle during negotiations on the planned digital trade chapter in the failed Transatlantic Trade and Investment Partnership (TTIP).

3. The Tangled Web of International Data Transfer Regimes

Current US law contains no general restrictions on the international transfer of personal data originating in the United States. Comprehensive privacy legislation considered in the last US Congress did not envisage fundamentally changing this laissez-faire approach,[23] and the next legislative effort in this area is unlikely to either.[24]

The EU's General Data Protection Regulation (GDPR), by contrast, conditions data flows from its territory on the existence of privacy safeguards that travel with the data. If the European Commission has decided that a particular third country ensures an "adequate" level of protection, data may flow freely to it from EU territory without additional formalities. For all other destinations, safeguards must be included in individual data transfer commercial contracts (standard contractual clauses, or SCCs).

The EU has gradually increased the number of adequacy findings it has issued enabling unrestricted data flows to favored countries, but the results remain relatively modest. The European Commission has issued fourteen unilateral adequacy findings in twenty-five years of effort[25] and has concluded three digital trade agreements.[26] As a result, a large proportion of data transfers between Europe and the rest of the world require the painstaking inclusion of privacy protection clauses in data transfer transactions.

22. Free Trade Agreement between the European Union and New Zealand, arts. 12.5 and 25.1.2.
23. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2021-2022), June 21, 2022, https://www.congress.gov/bill/117th-congress/house-bill/8152.
24. Congress did, however, introduce reciprocity as a requirement for law enforcement data transfers pursuant to the CLOUD Act and as part of eligibility criteria for access to the new Data Privacy Review Court established by Executive Order 14086. See: "DIVISION V: CLOUD ACT," Department of Justice, accessed May 13, 2023, https://www.justice.gov/criminal-oia/page/file/1152896/download and "Enhancing Safeguards."
25. The benefiting jurisdictions are Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, and Uruguay.

By one count, there now are 145 countries around the world with national data protection laws, many formally modelled on the EU's GDPR.[27] Seventy-three apply, at least in principle, the EU's conditional approach to international transfers.[28] The laws contain varying criteria for adequacy, however, and these countries' adequacy decisions do not necessarily track with those of the European Commission. While the European Commission decides on adequacy only after extensive and lengthy examination of a foreign privacy regime, some countries, for example Russia, regard simple adherence to the Council of Europe's (CoE's) multilateral privacy convention as conclusive evidence of adequacy.

The global result is a varying and inconsistent web of national determinations. Colombia, for example, finds data transfers from its territory to the United States to be adequately protected, whereas in Europe, the CJEU has twice struck down the European Commission's adequacy findings for the United States.[29] Other countries appear hesitant to use their adequacy powers at all for fear of angering large trading partners such as China.

4. EU-US Data Transfer Reconciliation

Washington and Brussels have tried repeatedly to settle their differences over data transfers. The European Commission, despite suffering two consecutive losses at the CJEU in challenges to adequacy findings for the United States, promptly returned to the negotiating table with Washington in 2020 for a third try. The result was the 2022 EU-US Data Privacy Framework (DPF), which the European Commission has proposed to find adequate. After the Council of the European Union expresses its view, the commission is expected to give final approval by the summer.

The DPF, like its predecessors, represents a compromise between the European and US approaches to data privacy. The EU would permit unrestricted transfers of personal data from EU territory to the United States on the basis that the agreement's privacy protections are essentially equivalent to those in the GDPR and EU fundamental rights law. The United States would enforce the agreed data protection measures through its own administrative agencies. Critics argue that the safeguards do not fully measure up, however, particularly in the areas of judicial redress and proportionality,[30] and a third challenge before the CJEU is all but certain. Although the DPF reflects a substantial effort by the United States to address criticisms of its surveillance law regime previously lodged by the CJEU, it may yet fall short in a further challenge.[31] Failure of the United States to adopt a comprehensive privacy law also could weigh in the court's consideration.

Until a new adequacy decision is issued, companies transferring personal data from EU territory to the United States largely rely on SCCs. Over the past two years, data protection authorities in several EU member states have found SCC safeguards insufficient to prevent the risk that US national security and law enforcement authorities might obtain transferred data. Their decisions have cast doubt on the ability of US cloud providers to offer certain services in Europe.[32] On May 22, the Irish Data Protection Commission imposed on Meta the largest-ever GDPR fine (€1.2 billion), ruling that the SCC safeguards it had put in place for its social network-related data transfers to the United States did not remove the risk of US government surveillance.[33]

US President Joe Biden gives a joint press statement in Brussels with European Commission President Ursula von der Leyen, announcing the EU-US Data Privacy Framework in principle. March 25, 2022. REUTERS/ Evelyn Hockstein

26. The three are Chile, New Zealand, and the UK.
27. Anupam Chander and Paul M. Schwartz, "Privacy and/or Trade," *University of Chicago Law Review* 90 (2023): 19, 10.2139/ssrn.4038531.
28. Joe Jones, "Global adequacy capabilities," IAPP (International Association of Privacy Professionals), last updated April 2023, https://iapp.org/resources/article/infographic-global-adequacy-capabilities/.
29. The first loss came in the 2015 Schrems I case challenging the Safe Harbor Framework and the second in the 2020 Schrems II case relating to the successor Privacy Shield. See: Maximillian Schrems v. Data Protection Commissioner, Judgment of the Court (Grand Chamber), October 6, 2015, Case C-362/14, Schrems, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN; Facebook Ireland Ltd., Maximillian Schrems, intervening parties: the United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance Inc., Digitaleurope, Judgment of the Court (Grand Chamber), July 16, 2020, Case C-311/18, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404.
30. See European Parliament's resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework. European Parliament, MEPs against greenlighting personal data transfers with the US under current rules, press release, April 13, 2023, https://www.europarl.europa.eu/news/en/press-room/20230411IPR79501/meps-against-greenlighting-data-transfers-with-the-u-s-under-current-rules.
31. Christopher Kuner, "International Data Transfers after Five Years of the GDPR: Postmodern Anxieties," EU Law Live, May 5, 2023, https://eulawlive.com/op-ed-international-data-transfers-after-five-years-of-the-gdpr-postmodern-anxieties-by-christopher-kuner/.
32. Google Analytics has been a particular target, for example in France. "Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply," CNIL, February 10, 2022, https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply.
33. Irish Data Protection Commission, "Data Protection Commission announces conclusion of inquiry into Meta Ireland, May 22, 2023, Data Protection Commission announces conclusion of inquiry into Meta Ireland | 22/05/2023 | Data Protection Commission.

Some major foreign cloud companies have, understandably, reacted to the increasingly hostile climate for transatlantic data transfers by deciding to localize their services in Europe. They have built new data centers in EU member states, promising customers that their data will not be transferred to the United States. A number have entered into formal joint ventures with European companies to further localize their presence.[34]

Despite this uncertainty, however, transatlantic data transfers have continued largely unabated, as they are simply too integral to digital commerce. Washington and Brussels, having expended great effort in recent years to create greater legal stability, now may be inclined to put the topic aside while awaiting the results of an anticipated third judicial challenge. But a wait-and-see attitude only invites a recurrence of bilateral crisis diplomacy. Instead, it is the right time for the United States and the EU to build on their achievements by broadening efforts toward a more sustainable transatlantic and global architecture for data transfers.

5. New Bilateral Directions

TTIP's demise was a missed opportunity, from the Obama administration's perspective, to embed guarantees for transatlantic data flows in trade law, but it need not be the last word. The United States and the EU could revisit the subject in a stand-alone digital trade negotiation, taking into account intervening agreements both have reached with other trading partners. In addition, they could utilize the now-established TTC as a forum for identifying and enhancing common features—particularly the concept of accountability—underlying their respective data privacy governance systems.

a. A bilateral electronic commerce accord?

The failure of TTIP negotiations left the United States and the EU without a bilateral trade framework for protecting and promoting data flows. In the intervening years, the EU has reached trade accords addressing electronic commerce with several Asian countries, including Japan and, most recently, New Zealand. The United States also concluded a digital trade agreement with Japan[35] and a digital trade chapter in the United States-Mexico-Canada Agreement (USMCA).[36]

The EU's Japan and New Zealand agreements do not address the interaction of data flows and privacy law in a way that the US government would find entirely satisfactory. The EU rebuffed Japan's bid for a binding commitment on the free flow of data, agreeing only to revisit the subject in the future.[37] The New Zealand accord contains only a soft exhortation to "ensuring cross-border data flows to facilitate trade in the digital economy and recognis(ing) that each Party may have its own regulatory requirements in this regard."[38] Both agreements do contain specific obligations restricting data localization measures, however.

The United States and the EU could profitably revisit the subject of electronic commerce, taking as a starting point the provisions that tentatively had been agreed in TTIP, as well as the more recent agreements both have reached with third countries. Prohibiting forced localization of data could be a common starting point. In addition, European Commission trade officials periodically have privately hinted that the bloc's insistence on an unrestricted privacy exemption to data flows could be ripe for revisiting.

There are precedents in WTO law that the United States and the EU could draw upon for potential compromises. For example, the WTO Understanding on Commitments in Financial Services precludes parties from preventing transfers of financial information, while allowing them to protect personal data "so long as such right is not used to circumvent the provisions of the agreement"—a so-called non-circumvention provision.[39] Washington and Brussels also could look for inspiration to the WTO's GATS, which allows parties to pursue public policy objectives such as privacy, provided the measure does not constitute "arbitrary or unjustifiable discrimination or a disguised restriction on trade" or restrict information transfers to a greater extent than necessary to protect privacy.[40] Limiting provisions such as these would be valuable protections in themselves for data transfers, even if the United States is not able to achieve with the EU the fuller obligations in this area contained in, for example, the USMCA.[41]

b. Putting the TTC to work on data transfers

The US government and the European Commission could utilize the TTC as a first step toward developing common

34. Microsoft, for example, has created a new joint venture, Bleu, with French companies Orange and Capgemini. Jean-Philippe Courtois, "Powering critical infrastructure with Microsoft cloud technology," Microsoft, May 26, 2021, https://blogs.microsoft.com/blog/2021/05/26/powering-critical-infrastructure-with-microsoft-cloud-technology/.
35. "US-Japan Digital Trade Agreement Text," Office of the United States Trade Representative, accessed May 13, 2023, https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text.
36. "Chapter 19: Digital Trade" in United States-Mexico-Canada Agreement, accessed May 13, 2023, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.
37. Agreement between the European Union and Japan for an Economic Partnership, art. 8.81, accessed May 13, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02018A1227(01)-20220201&from=EN#bm306level1.
38. "EU-New Zealand: Text of the agreement," European Commission, art. 12.4, accessed May 13, 2023, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement_en.
39. "Understanding on commitments in financial services," World Trade Organization, accessed May 13, 2023, https://www.wto.org/english/tratop_e/serv_e/21-fin_e.htm.
40. General Agreement on Trade in Services, art. XIV.
41. Agreement between the United States of America, the United Mexican States, and Canada, art. 19.11.

US Secretary of State Antony Blinken, US Secretary of Commerce Gina Raimondo, European Commission Executive Vice-President Margrethe Vestager and European Commission Executive Vice-President Valdis Dombrovskis speak at the third Trade and Technology Council meeting in College Park, Maryland. December 5, 2022. REUTERS/Saul Loeb/Pool

thinking on data transfers and privacy. The TTC, established in 2021, periodically brings together political leadership and experts from Washington and Brussels. It already has yielded shared approaches on subjects as varied as technology-related export controls and assessing risks associated with artificial intelligence. One of the TTC's ten standing working groups (Working Group 5) is charged with data governance issues; its mandate is "to exchange information on our respective approaches to data governance and technology platform governance, seeking consistency and interoperability where feasible."[42] This mandate appears broad enough to encompass data transfers and privacy, or alternatively, a new group could be assembled to address this topic.

Despite lacking a comprehensive national privacy law comparable to the EU's GDPR, the United States does have an array of federal-level sectoral privacy laws, a burgeoning number of state-level privacy laws, and a series of international agreements on data transfers, particularly in the law enforcement and security area. One common concept already linking European and US approaches to privacy regulation is that entities controlling individuals' personal data must be proactively accountable for it. That is, they must assess the risks associated with their data handling, put in place internal policies and mechanisms for managing it safely, and provide evidence of compliance to external stakeholders, including supervisory authorities. The concept of accountability appears not only in the GDPR but also in a series of international law instruments relating to data flows and privacy.[43]

Europe's data protection authorities have produced detailed guidance for companies on assessing risks of foreign government surveillance of transferred data and instituting attendant safeguards via standard contract clauses.[44] The United States thus far has not embraced a comparable precautionary approach to the privacy risks of international data transfers, but, as it moves toward a comprehensive federal privacy law and toward expanded engagement on data transfers in multilateral settings, it inevitably will be pushed in this direction.

The TTC could be utilized to explore and deepen a common transatlantic direction on privacy risk assessment. The body's past success in developing the AI Joint Roadmap,[45] which addresses other sorts of technological risk, offers an instructive precedent. Participants in privacy risk discussions should include officials responsible for digital trade as well as privacy regulators, bolstered as necessary by experts from the law enforcement and national security communities. Such an exercise would be bureaucratically complex since some of these actors do not currently participate in the already elaborate TTC structure. But expert-level engagement on privacy risk could yield common thinking of more than commensurate value.

6. Toward a more coherent multilateral data flow regime

Bilateralism is not the only avenue for finding a durable solution to international data flow difficulties. There are a variety of multilateral organizations in which the United States and

42. Office of the United States Trade Representative, "Working Group 5 - Data Governance and Technology Platforms" in "US-EU Trade and Technology Council Inaugural Joint Statement," September 29, 2021, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/september/us-eu-trade-and-technology-council-inaugural-joint-statement.
43. See, for example, EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), arts. 5(2) and 24, *Official Journal of the European Union*, May 4, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504; "OECD Privacy Principles," OECDPrivacy.org, accessed May 13, 2023, http://oecdprivacy.org/; and APEC Privacy Framework (Singapore: APEC Secretariat, 2015), https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf.
44. "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures," European Data Protection Board, November 10, 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.
45. Office of the United States Trade Representative, "US-EU Joint Statement of the Trade and Technology Council," December 5, 2022, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/us-eu-joint-statement-trade-and-technology-council.

the EU participate that could serve as potential negotiating fora. They range from the WTO, with its ongoing e-commerce negotiations, to European and Asia-Pacific regional organizations—the Organisation for Economic Co-operation and Development (OECD), CoE, and the Asia-Pacific Economic Cooperation (APEC)—with established records in the privacy area. In multilateral settings, US and EU differences need not dominate discussions. Other countries with strong ambitions to devise a more workable data transfer architecture, including Australia, Japan, New Zealand, South Korea, and the UK, can take on principal negotiating roles.

a. The World Trade Organization to the rescue?

In 2017, seventy-one WTO members decided to explore prospects for a WTO agreement on trade-related aspects of electronic commerce. Actual negotiations commenced two years later and continue to this day.[46] Additional WTO members have joined the plurilateral talks, so that more than eighty now participate.

Progress in the talks has been slow. Both the United States and the EU have put forward proposals on this topic that are drawn from their bilateral and regional agreements.[47] The EU, for example, proposes to bar data localization requirements but not other types of data flow restrictions, and to incorporate a self-judging privacy exception.[48]

Since WTO trade negotiations operate by consensus, a lowest-common-denominator outcome to the e-commerce talks seems eventually likely. The parties may well agree on a series of provisions unrelated to data flows, such as facilitating the use of electronic contracts, and leave more contentious issues to the side. The prospect of a near-universal WTO accord settling the question of data flows and privacy appears to be modest, at least for the near term.

However, some observers believe that the WTO still can serve as the setting for a binding international agreement on trans-border data flows, if the hard work of reconciling diverse privacy perspectives is outsourced to a specialist organization. One option, they suggest, would be the Global Privacy Assembly (GPA), a forum for privacy regulators from eighty-two countries.[49] The GPA already has begun to explore common principles underlying national privacy rules.[50]

The European approach dominates at the GPA, and the United States—lacking a fully empowered national privacy regulator—is only an observer at the organization.[51] Engaging the GPA to develop substantive privacy protection norms underpinning free data flows conceivably could hold promise as a way of eventually overcoming the current deadlock in the WTO e-commerce negotiations, where reflexive positions thus far have prevailed. But the United States likely would remain wary of the GPA assuming such a consequential role, at least until it passes comprehensive privacy legislation and empowers a national-level privacy regulator with comparable powers to European counterparts.

b. Regional Approaches

Modest prospects for resolution of the data flow and privacy impasse at the WTO do not necessarily doom all multilateral efforts. Rather, there are several regional international organizations with more limited memberships which could serve as useful avenues for discussion and reconciliation.

OECD: The Paris-based OECD, made up of thirty-eight developed countries, has long been an important international actor on data flows and privacy. Most OECD members are Europe-

President of the European Council Charles Michel welcomes Director-General of the World Trade Organization Ngozi Okonjo-Iweala before a meeting in Brussels, Belgium. May 19, 2021. REUTERS/John Thys/Pool

46. "Joint Statement on Electronic Commerce," World Trade Organization, January 25, 2019, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/1056.pdf&Open=True.
47. Chander and Schwartz, "Privacy," 49.
48. EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, 26 April 2019. directdoc.aspx (wto.org). Also see, European Parliament Research Service, "WTO e-commerce negotiations," European Parliament, October 2020, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf. The European Parliamentary Research Service study states: "The EU proposal seeks to balance the free flow of data for business purposes with a commitment to personal privacy, which it considers a fundamental right. Enterprises should not be restricted by requirements to localise data or computer facilities in a given member's territory."
49. Chander and Schwartz, "Privacy," 50.
50. Elizabeth Denham, "Solving the billion-dollar question: how do we build on the foundations of convergence?" GPA (Global Privacy Assembly), November 1, 2021, http://globalprivacyassembly.org/solving-the-billion-dollar-question-how-do-we-build-on-the-foundations-of-convergence/.
51. The Federal Trade Commission, an independent agency, represents the United States at the GPA and engages to the extent permitted by its status as an independent non-executive body and by the limits of its consumer protection authorities.

an countries, but the body also includes other major economies from Asia, North America (including the United States), Latin America, and the Middle East. The European Commission participates as an observer.[52] The OECD's "Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data," issued in 1980 and updated in 2013,[53] are a widely recognized standard for protecting privacy interests in personal data transferred internationally for commercial purposes. Although the guidelines are nonbinding "soft law," they nonetheless have had broad influence on members' national privacy legislation.

The OECD guidelines do not attempt to reconcile the tension between privacy and government access to data; instead, they simply allow members to define their own exceptions for "national security and public policy."[54] As public concerns over foreign intelligence and law enforcement surveillance grew in the past decade, the OECD worked to further define the permissible scope of such activities.[55] In December 2022, the OECD issued its Declaration on Government Access to Personal Data Held by Private Sector Entities. It took two years of low-key, non-public negotiations among members' national security and law enforcement, privacy, and diplomatic officials to conclude.[56]

The declaration is an effort to capture the "significant commonalities" characterizing how "rule of law democratic systems" already regulate their access to personal data in the possession of private sector entities such as communications companies. As the OECD notes, it is "the first intergovernmental agreement" on the subject, albeit a nonbinding one.[57] In effect, the OECD declaration serves as a confidence-building measure by describing its members' existing protections.

The declaration's seven principles adapt traditional concepts for protecting privacy in the commercial setting to the sensitive setting of national security and law enforcement access. They describe, for example, how governments tailor access demands to what is necessary and proportionate, and how they structure prior approval processes, transparency regimes, and oversight and redress mechanisms.

US State Secretary Blinken and OECD Secretary-General Cormann speak at an OECD Ministerial in Paris, France. October 6, 2021. REUTERS/Ian Langsdon/Pool

Although the declaration is a significant step forward in shedding light on the shadowy world of government surveillance safeguards, it is far from the last word on articulating rule of law considerations in this area. For example, OECD governments were not prepared to discuss extraterritorial "direct" access—data acquisition not involving private sector entities—nor other controversial practices such as purchasing databases from the private sector. In addition, the distilled principles are not accompanied by a comprehensive catalogue documenting the legal specifics of members' actual government access regimes.[58]

Nonetheless, the OECD declaration on government access could serve as the foundation for a further legal instrument in which governments commit that their national security and law enforcement agencies will adhere to these principles—and provide detailed information on how their laws enable them to do so. The OECD could invite non-members to subscribe to the declaration and to document their compliance.

In other words, OECD members could move beyond a descriptive legal instrument to a prescriptive one. Such an agreed document need not be binding as a matter of international law; rather, it could take its place in the constellation of OECD soft law instruments. Jurisdictions such as the EU that condition international data flows on the existence of sufficient

52. Although not a voting member of the OECD, the European Commission often exercises outsize influence by coordinating positions among its member states. "European Union and the OECD," OECD, accessed May 13, 2023, https://www.oecd.org/eu/european-union-and-oecd.htm.
53. "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," OECD, as amended on July 11, 2013, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.
54. Ibid., para. 4.
55. The Data Free Flow with Trust initiative, initially proposed by Japan during its Group of Twenty presidency in 2019, was an important stimulus to the OECD's work on this topic. "Speech by Prime Minister Abe at the World Economic Forum Annual Meeting," Ministry of Foreign Affairs of Japan, January 23, 2019, https://www.mofa.go.jp/ecm/ec/page4e_000973.html.
56. Kenneth Propp, "Gentlemen's Rules for Reading Each Other's Mail: The New OECD Principles on Government Access to Personal Data Held by Private Sector Entities," *Lawfare*, January 10, 2023, https://www.lawfareblog.com/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held.
57. "Background information" in "Declaration on Government Access to Personal Data held by Private Sector Entities," OECD Legal Instruments, accessed May 13, 2023, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.
58. Propp, "Gentlemen's Rules."

Foreign ministers from the Council of Europe member states pose for family photo in Venaria Reale, near Turin, Italy. The United States is an observer at the CoE. May 20, 2022. REUTERS/Massimo Pinca

safeguards related to government access then could accept adherence to these elaborated rule of law principles as a sufficient basis to allow free data flows.

Council of Europe: The CoE, Europe's oldest human rights organization, also has a long history of codifying privacy protection into international law. Its 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[59] was updated in 2018 and dubbed Convention 108+.[60] Convention 108+ sets standards for the CoE's forty-five European members, as well as for ten other non-European countries which have acceded to it.[61]

The CoE's Convention 108+, unlike the OECD's privacy-related instruments, is binding as a matter of international law; it lacks a strong enforcement mechanism, however. Parties to Convention 108+ are generally obliged to allow trans-border data transfers to the territories of other parties.[62] Convention 108+ also is closely linked to EU law, mirroring the GDPR in many respects, albeit at a greater level of generality. Although the EU does not regard adherence to Convention 108+ as conclusive proof of a country's adequacy for purposes of international data transfers under the GDPR, the European Commission does regard it as a factor that "should be taken into account."[63] Adherence to Convention 108+ has yet to significantly influence commission adequacy decisions, however.

The United States, an observer state at the CoE, has not acceded to Convention 108+, although it has selectively joined other CoE legal instruments, including its successful Convention on Cybercrime.[64] The CoE periodically has encouraged the United States to consider joining Convention 108+, but doing so would require changes to US law that Washington has been unwilling to entertain. For example, Article 15 requires that a party have a supervisory data protection authority along the lines of the GDPR. If the United States adopts a comprehensive federal privacy law, it conceivably could satisfy this and other Convention 108+ requirements. Congress could include in such legislation a provision encouraging the president to consider accession to Convention 108+.

In 2020, the chair of the CoE's Convention 108+ committee proposed that the organization undertake work addressing government access to data.[65] However, the proposal did not advance, eclipsed by the OECD's parallel effort. Any future CoE work on this topic is likely to be complementary to the OECD declaration.

59. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No. 108, Council of Europe, January 28, 1981, https://rm.coe.int/1680078b37.
60. *Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data*, Council of Europe, June 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
61. "Details of Treaty No. 108," Council of Europe, accessed May 13, 2023, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.
62. *Convention 108+*, art. 14.
63. EUR-Lex, EUR-Lex, Regulation (EU) 2016/679, Recital 105.
64. "Council of Europe – Convention on Cybercrime (ETS No. 185) – Translations," Council of Europe, November 23, 2001, https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations.
65. "Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services," joint statement by Alessandra Pierucci, chair of the Committee of Convention 108, and Jean-Philippe Walter, data protection commissioner of the Council of Europe, September 7, 2020, https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb.

The G7 heads of state attend a meeting during the G7 Leaders' Summit in Hiroshima. The summit endorsed the Ministerial Declaration which promoted the Data Free Flow with Trust initiative. May 19, 2023. REUTERS/Brendan Smialowski/Pool

Data Free Flow with Trust: The Group of Seven (G7) and Group of Twenty (G20) countries also have focused in recent years on international data transfers. These groups can serve as incubators for new thinking and can provide an impetus for institutionalizing further work in existing regional international organizations.

In 2019, the G20 endorsed a proposal by then Japanese prime minister Shinzo Abe to make "data free flow with trust" (DFFT) a guiding principle for cross-border data transfers.[66] DFFT is a slogan that suggests a prospect of harmony between open data flows and privacy protection.

It is no accident that Japan launched the DFFT initiative on the heels of its lengthy and difficult—but ultimately successful—quest to obtain an EU adequacy finding.[67] Japan also has concluded a digital trade agreement with the United States containing data flow guarantees.[68] Japan sees itself as a pragmatic broker in the multilateral arena between the US and EU perspectives.

Since its 2019 launch, there has been work under the DFFT rubric in several international contexts. The World Economic Forum has prepared studies identifying data transfer obstacles faced by companies.[69] In 2021, the G7 digital and technology ministers issued a DFFT road map identifying data localization, cross-border regulatory cooperation, and data sharing as particular areas requiring common approaches.[70] In 2022, the OECD issued the aforementioned Declaration on Government Access to Personal Data Held by Private Sector Entities.[71] Recently, the OECD released an analysis of business experiences with international data flows.[72]

66. "G20 Osaka Leaders' Declaration," Ministry of Foreign Affairs of Japan, accessed May 13, 2023, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.
67. South Korea is the only other country with both EU adequacy findings and a digital trade agreement with the United States.
68. In addition, Japan has an Economic Partnership Agreement with the EU, but it does not contain a comparable provision on unrestricted data flows. "Agreement between the European Union and Japan for an Economic Partnership," Ministry of Foreign Affairs of Japan, accessed May 13, 2023, https://www.mofa.go.jp/files/000382106.pdf.
69. World Economic Forum, *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*, June 10, 2020, https://www.weforum.org/whitepapers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows.
70. G7 Research Group, University of Toronto, "Ministerial Declaration, G7 Digital and Technology Ministers," April 28, 2021, http://www.g7.utoronto.ca/ict/2021-digital-tech-declaration.html.
71. "Declaration on Government Access to Personal Data Held by Private Sector Entities," OECD Legal Instruments, December 13, 2022, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.
72. OECD, "Moving forward."

Japan is using its current G7 presidency to further pursue DFFT. In April, G7 digital and technology ministers "recognise(d) the need to accelerate and operationalise work on DFFT." The Ministerial Declaration added that the G7 seeks to "build upon commonalities, complementarities, and elements of convergence between existing regulatory approaches and instruments.... [W]hile recognising our varied approaches to data governance."[73] The G7 heads of state endorsed the Ministerial Declaration at their summit in Hiroshima in May.[74]

G7 digital ministers announced the creation in the coming months of an Institutional Arrangement for Partnership (IAP), consisting of governments and stakeholders, to develop compatible policies and practices for enabling data flows. They identified the OECD as the institutional locus for ongoing DFFT work, including further developing the OECD declaration on government access to data, and finding consensus approaches to data sharing in priority sectors including health care and climate. IAP also could launch pilot projects exploring technological solutions such as privacy enhancing technologies; corporate stakeholders would play a role in designing the projects.[75]

Washington and Brussels have cautiously embraced DFFT. Japan's success in institutionalizing the topic at the OECD while steering clear of transatlantic philosophical disagreements thus is an encouraging development. Over the medium term, combining the DFFT political impetus with the OECD's institutional strengths could become a significant driver of a more coherent international context for data flows.

Globalizing the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules: Although European governments historically have been most comfortable relying on a Europe-based regional organization to find a durable solution to the privacy problem in international trade, other multilateral bodies also could fill the role. The United States has long promoted an alternative—the Cross-Border Privacy Rules (CBPR) System developed by the Asia-Pacific Economic Cooperation (APEC) in 2005 and updated in 2019.[76]

The CBPR is designed to serve as a legal basis for international data transfers. Governments and companies voluntarily participate in it. Australia, Canada, Japan, Mexico, the Philippines, Singapore, South Korea, Taiwan, and the United States have joined.[77] Companies self-certify their compliance with the CBPR's privacy standards and agree to submit to the scrutiny of an independent external auditor. It is premised on the concept of accountability, under which companies self-assess data transfer risks and put appropriate safeguards in place, subject to external review by an accountability agent.

Despite its business-friendly design, the CBPR System has struggled to reach critical mass, with only a small number of major multinational companies, including Google, utilizing it. The European Commission has long been skeptical about the APEC CBPR because of its variance from the GDPR model for protecting data transfers. Past discussions between APEC governments and the commission on comparing and linking the two approaches have not been productive.

To achieve broader scale, seven of the APEC CBPR governments announced in April 2022 that they intended to transform it into a global system. They established a Global CBPR Forum, an umbrella entity that would "help bridge different regulatory approaches to data protection and privacy."[78] In April 2023, the forum issued an open invitation for countries to join,[79] as well as a detailed framework and terms of reference. The CBPR forum boasts international heft, with four G7 countries[80] as well as four of the Five Eyes countries[81] participating. The UK has filed an application to join.[82]

The forum held a workshop in London in April, with more than twenty governments from across Asia, the Middle East, Europe (not including the EU), and the Americas attending. They discussed the reforms to the original CBPR agreement, as

73. "Ministerial Declaration the G7 Digital and Tech Ministers' Meeting," G7 2023, Hiroshima Summit, April 30, 2023, https://g7digital-tech-2023.go.jp/topics/pdf/pdf_20230430/ministerial_declaration_dtmm.pdf.
74. G7 Hiroshima Leaders' Communique, May 20, 2023, Data Protection Commission announces conclusion of inquiry into Meta Ireland | 22/05/2023 | Data Protection Commission.
75. "G7 Digital and Tech Track: Annex 1: Annex on G7 Vision for Operationalising DFFT and its Priorities," G7 Digital and Tech Ministers' Meeting in Takasaki, Gunma, April 29-30, 2023, April 30, 2023, https://g7digital-tech-2023.go.jp/topics/pdf/pdf_20230430/annex1.pdf.
76. "APEC Cross-Border Privacy Rules System," Cross-Border Privacy Rules System, updated November 2019, http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf.
77. "Government," Cross-Border Privacy Rules System, accessed May 13, 2023, http://cbprs.org/government/.
78. US Department of Commerce, Statement by Commerce Secretary Raimondo on Establishment of the Global Cross-Border Privacy Rules (CBPR) Forum, press release, April 21, 2022, https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border.
79. Global CBPR Forum, "Global Cross-Border Privacy Rules (CBPR) Forum Welcomes Participation by Interested Jurisdictions," April 13, 2023, https://www.globalcbpr.org/global-cross-border-privacy-rules-cbpr-forum-welcomes-participation-by-interested-jurisdictions/?mkt_tok=MTM4LUVaTS0wNDIAAAGLIB_NNzEGJKRZII_SkOWHF8S4N8xXaz-S1VaPWUA0qAbcElsz7DTILwXVwpNhlrN_WI3ShyRZZMWkLBY6-dDRx5NrCnmtTqe0PpZ3Ar181dSzF.
80. The four G7 countries are Canada, Japan, the United Kingdom, and the United States.
81. The four 5 Eyes countries participating are Australia, Canada,the United Kingdom, and the United States.
82. International Trade Administration, Commerce Department welcomes UK's application to the Global CBPR Forum, press release, April 17, 2023, https://www.trade.gov/press-release/commerce-department-welcomes-uks-application-global-cbpr-forum.

US Vice President Kamala Harris speaks with Prime Minister of Thailand Prayut Chan-o-cha at the Asia-Pacific Economic Cooperation (APEC) summit at Queen Sirikit National Convention Center in Bangkok, Thailand. Nov. 19, 2022. REUTERS/Haiyun Jiang/Pool

well as internal governance changes to reflect its new global cast.[83] A second meeting is planned in Brazil in the fall.

Governments participating in the Global CBPR System reportedly are considering strengthening the agreement's privacy safeguards. One step could be to establish a linkage to the OECD declaration as a way of demonstrating the CBPR's seriousness about government access. Such a link could help alleviate EU skepticism about the CBPR initiative. Some governments with active national security surveillance programs (including the United States) may be reluctant to commit to such additional safeguards, however. Nonetheless, the Global CBPR System eventually could become a relevant feature in the international data transfer landscape, particularly if more governments recognize it in their domestic laws as a lawful basis for international data transfer.

Indo-Pacific Economic Framework for Prosperity: The Biden administration has launched discussions with a number of Asian allies (Australia, Brunei Darussalam, Fiji, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Thailand, and Vietnam) on "open trade commitments" including "trusted and secure cross-border data flows."[84] The Office of the US Trade Representative has publicly confirmed that data protection issues also are part of the discussions.[85] Press reports suggest that the draft data flow provisions under negotiation resemble those in the USMCA, but with larger public policy exceptions.[86]

It is too soon to know whether these discussions eventually could result in binding obligations similar to those contained in the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). The Biden administration thus far has proven to be unwilling to contemplate new comprehensive free trade agreements. Discussions in the Indo-Pacific Economic Framework for Prosperity suggest, however, that it at least is considering the utility of a subset of commitments in the digital economy area.

83. Mark Scott, "Digital Bridge: Global AI rulebook — US digital policymaking — Data rules," *Politico*, April 20, 2023, https://www.politico.eu/newsletter/digital-bridge/global-ai-rulebook-us-digital-policymaking-data-rules/?utm_source=POLITICO.EU&utm_campaign=383dcc1730-EMAIL_CAMPAIGN_2023_04_20_11_30&utm_medium=email&utm_term=0_10959edeb5-383dcc1730-%5BLIST_EMAIL_ID%5D.
84. "Ministerial Text for the Trade Pillar of the Indo-Pacific Economic Framework for Prosperity," Office of the United States Trade Representative, September 9, 2022, https://ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text%20(Trade%20Pillar)_FOR%20PUBLIC%20RELEASE%20(1).pdf.
85. "Pillar I: Trade," Office of the United States Trade Representative, accessed May 13, 2023, https://ustr.gov/sites/default/files/2023-04/IPEF%20Pillar%201%20text%20summaries%20USTR%20April%202023.pdf.
86. Cristiano Lima and David DiMolfetta, "Big Tech trying to 'weaponize' US trade talks, Democrats warn," *Washington Post*, April 24, 2023, https://www.washingtonpost.com/politics/2023/04/24/big-tech-trying-weaponize-us-trade-talks-democrats-warn/.

Conclusion

The transatlantic "privacy problem," narrowly conceived, is how to fashion stable governance arrangements enabling personal data to move efficiently between Europe and the United States, while creating confidence that national security and law enforcement agencies' access to transferred data is subject to rule of law disciplines. The new EU-US DPF and the OECD declaration are important building blocks toward trust.

Viewed more broadly, however, one can see the competing perspectives offered by trade and consumer law, human rights law, and, increasingly, national security law. Each perspective carries a different emphasis. The US government, viewing data flows principally as integral to commerce, has long preferred the structures of trade law—bilateral, regional, and global—as the predominant solution. But its abandoned attempts to reach regional trade agreements in the Atlantic or Pacific reveal the limits of betting on trade law to secure data flows. More likely, the United States will seek progress on the margins, through bilateral digital trade agreements or looser commitments with like-minded jurisdictions.

In Europe, data protection law, which first emerged as a specialized branch of human rights law, continues to dominate thinking about data transfers. Although the EU's GDPR formally recognizes the economic importance of international data flows, the steady drumbeat of the CJEU and national data protection authorities' restrictive rulings has demonstrated a readiness to disrupt international commerce if predicate transfer safeguards do not remove the risk of foreign surveillance.

The newest perspective, emerging in parallel on both sides of the Atlantic, would limit international data flows for national security reasons. Whether the question is allowing Chinese social media companies to transfer foreign-origin data back to China or corporate data flows to outcast Russia, the emerging answer is the same: data flows take a back seat to geostrategic concerns.

As these approaches collide, the obvious danger is legal fragmentation.[87] The EU will persist in viewing its adequacy and contractual clause tools as the basis for a global data governance order. The United States will press, increasingly hesitantly, trade solutions. And both sides delicately will acknowledge their growing consciousness of national security risks in data transfers.

Recent years have seen a profusion of international actors bidding to regulate this space. From APEC to the CoE to the OECD to the WTO to the G7—an alphabet soup of ambitious and, to some extent, competing initiatives has emerged. The proliferation of fora is a positive development, offering a fertile environment where perspectives can confront one another and comingle.[88] The building blocks for a more coherent data transfer architecture are there, though how they will fit together remains unclear. The next years will be messy, but, perhaps, ultimately fruitful.

87. Kuner, "International Data Transfers."
88. Paul Schiff Berman, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* (Cambridge University Press, 2012), 10.

About the author

Kenneth Propp is a nonresident senior fellow with the Atlantic Council's Europe Center and an adjunct professor of European Union Law at the Georgetown University Law Center and a senior fellow with the Cross-Border Data Forum. He advises and advocates on data trade, privacy, security, and other regulatory issues in the United States and major international markets. From 2011-2015, he served as legal counselor at the US Mission to the European Union in Brussels, Belgium, where he led US Government engagement on privacy law and policy and digital regulation, and advised on trade negotiations with the EU. In previous assignments for the Office of the Legal Adviser, US Department of State, Propp specialized in legal issues relating to international criminal law and international trade and investment law. He also served as legal adviser to the US Embassy in Germany. Professor Propp holds a JD from Harvard Law School and a bachelor's degree from Amherst College.

Acknowledgements

The Atlantic Council's Europe Center would like to thank our sponsors, including Google and Amazon Web Services, for their support of our work. The Atlantic Council's partners are not responsible for the content of this report, and the Europe Center maintains a strict intellectual independence policy in line with the Atlantic Council Policy on Intellectual Independence.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Todd Achilles
Gina F. Adams
Timothy D. Adams
*Michael Andersson
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of April 18, 2023

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