Resolving the Conflict Between Trade and Data Protection Law

*Paul M. Schwartz and Anupam Chander**

The next decade will see increasing conflict between data privacy laws and international trade law. Governments are already concerned that privacy will be lost amid global data flows and have responded by enacting regulatory measures that might impede modern trade. While the European Union's findings of 'adequacy' offer a potentially trade-friendly solution to cross-border data flows, fewer than a dozen countries have been found adequate. In addition, more than sixty countries have enacted laws where they too evaluate the adequacy of foreign privacy laws. This splintering of data privacy law complicates global trade as more nations review and potentially restrict outbound data flows. New solutions are needed to ensure the benefits of trade while safeguarding privacy. This paper argues that a broad international agreement is needed that sets minimum standards, develops common regulatory language, and creates binding commitments in the context of data privacy and trade law.

Keywords: trade law, data protection law, World Trade Organization, adequacy finding, General Agreement on Trade in Services (GATS)

The future of data protection is one in which law and norms are numerous, growing in number, and fragmented in nature. Rather than a central law, such as the General Data Protection Regulation (GDPR), that provides a lodestone for regulated entities, the next decade will see myriad, overlapping, and sometimes contradictory statutes and regulations. Data protection generalists will race to keep up, and data protection subject matter specialists will struggle to see the forest for the trees.

In this rich regulatory landscape, one area is destined for increased importance. This area concerns the intersection of international data privacy and trade law. International trade is of central significance to both individuals and businesses. Trade supports more productive and higher paying jobs in export sectors, increases the range of products available to consumers and businesses, and keeps the economy dynamic and competitive.[1] Moreover, cross-border transfers are increasingly important for the global economy. Indeed, the 'ability to move, store and process data across borders is foundational to the modern international data economy.'[2] Consider the range of innovations that rely on the transfer of data across borders, such as the internet of things, the app economy, the outsourcing of services, e-commerce, cloud computing, big data, digital products and streaming services, social media, the sharing economy, and crowdfunding.[3]

At the same time, data protection law is more significant than ever before. A digital revolution is still underway and reaching into all domains of life. More of our devices are being tied to the internet, includ-

DOI: 10.21552/edpl/2023/3/6

* Paul M. Schwartz, Jefferson E. Peyser Professor of Law, Berkeley Law School. Anupam Chander, Scott K. Ginsburg Professor of Law and Technology, Georgetown Law School. For correspondence: <pschwartz@law.berkeley.edu>.

1 Office of the United States Trade Representative, 'Benefits of Trade' <https://ustr.gov/about-us/benefits-trade> accessed 13 September 2023.

2 World Economic Forum, *A Roadmap for CrossBorder Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy* (White Paper, 2020) 5.

3 Usman Ahmed and Anupam Chander, 'Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows' (2006) UC Davis Legal Studies Research Paper No. 480 <https://ssrn.com/abstract=2731888> accessed 13 September 2023.

ing even our toothbrushes and washing machines, and are generating finely grained details about our daily lives. At the same time, artificial intelligence is causing new kinds of privacy invasions. Cameron Kerry has explained,

> As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed.[4]

This essay explores the current and continued conflict between international privacy law and trade law. Data privacy became a policy issue a half-century ago with the advent of computerisation. As our lives have grown increasingly intertwined with digital products and services, the protection of information privacy has become increasingly urgent. It is not surprising, then, that data privacy laws have proliferated over the last few decades across the world. The next decade will see increasing conflict between data privacy laws and international trade, as governments worry that privacy might be lost amid global data flows.

This essay proceeds in three parts. First, it looks at the conflict between privacy and trade. In particular, trade law has delayed the tough decisions ahead about the integration of these two principles in the world's free trade system. Second, this essay explores the difficulties that this regulatory delay has caused. In particular, there are myriad 'adequacy' standards throughout the world for evaluation of the permissibility of a transfer of personal data, but no common definition of what this benchmark requires. Other areas of privacy law, such as the modalities of gaining consent, differ widely from country to country. Third, regarding solutions, this essay points to international developments that suggest the potential for a broad agreement around new rules to preserve privacy and promote global trade.

I. The Conflict

In earlier work, we have explored the tension between privacy and trade.[5] Countries across the world are now creating barriers to personal data travelling across borders. But trade in goods and services alike now require cross-border data flows. At the same time, moreover, the trade law that regulates services has created a regulatory thicket of divergent privacy rules inconsistently applied.

Our analysis begins with the General Agreement on Trade in Services (GATS). In creating GATS in 1994, governments inserted an open-ended, yet at least partially cabined, privacy exception in this treaty. GATS allows signatory nations to protect privacy when this action can be said to be 'necessary.' It neither establishes global minimum standards for privacy nor creates an international process for crafting such standards. We have called this exception for necessary privacy protections, the 'Privacy Bracket.'[6]

When negotiating GATS, signatory countries committed to liberalise trade in certain services by agreeing to provide market access and equal treatment to suppliers from other members of the World Trade Organization (WTO). In establishing GATS, the Uruguay Round of multilateral negotiations finalised a new international trade order that introduced services to the global trade rules. The Uruguay Round also established the WTO. GATS sought to create a stable climate for global trade and to promote competition and market liberalisation.

As for the Privacy Bracket, GATS sets it out along with general exceptions to its framework in its Article XIV. These exceptions, including the Privacy Bracket, allow signatory nations to adopt measures that would otherwise violate the treaty. The general exceptions include the protection of public order and human health as well as the prevention of fraudulent and deceptive practices. Article XIV(c)(ii) then expresses the Privacy Bracket. It states,

> [N]othing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures ... necessary to secure compliance with laws or regulations ... including those relating to: *the protection of the privacy of individuals in relation to the processing and dissemination of personal data.*[7]

This language excludes privacy laws from the new international trade regime for services.

4 Cameron Kerry, 'Protecting privacy in an AI-driven world' (*The Brookings Institution*, 10 February 2020) <https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world> accessed 13 September 2023.

5 Paul Schwartz and Anupam Chander, 'Privacy and/or Trade' (2023) 90 University of Chicago Law Review 49.

6 Ibid, 56.

7 General Agreement on Trade in Services 1995, art 14.

At the same time, however, GATS does not create a limitless exception for data privacy. If it did so, the risk would be that a signatory nation might claim to be regulating privacy, but actually be seeking to benefit one of its domestic industries. From today's perspective that danger is more than hypothetical. In America, observers have long criticised European data protection as motivated, at least in part, by protectionism. Their view is that the European Union is seeking to handicap American tech giants and to safeguard domestic industries.

GATS contains two restrictions on the Privacy Bracket, one that is general, and one that is specific. First, Article XIV begins with general limitations on all its exceptions; it makes them '[s]ubject to the requirement that such measures are not applied in a manner which would constitute a means or arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.' Second, the Privacy Bracket itself, as the quotation in the preceding paragraph indicates, adds the requirement that the adopted measure be 'necessary' for the protection of data privacy.

What has been the impact of the Bracket? Under GATS, the Privacy Bracket can be justified only under relatively stringent tests. A trade restriction made to protect privacy must be 'necessary' and cannot be a disguised restriction on trade. As a general rule, the determination of whether a trade restriction is necessary depends on whether there is a 'reasonably available' alternative that achieves the same policy goals while also creating lesser restrictions on trade. There must also be 'consistency of enforcement,' which means that a GATS signatory must not single out one state for stricter application of extraterritorial provisions in its data protection law.

To date, however, WTO tribunals have never policed the Bracket; that is, no privacy case has come before it. Through the WTO's Dispute Settlement Understanding, there is a process in place to complain about misuse of Article XIV(c)(ii), and scholars have argued that EU data protection should be viewed as problematic and not meeting the required 'consistency of enforcement.'[8] But no country has sought to test a potentially discriminatory use of the Privacy Bracket since the creation of GATS in 1995. This lack of privacy cases is especially surprising because many complaints have been raised before the WTO about violation of services trade commitments.

The bottom line is that GATS has pushed back to a later day hard decisions about how to integrate privacy and trade law in the world's free trade system. The result has been that numerous countries have enacted laws that limit cross-border data flows that originate from their territory.

II. The Problem

GATS contains a Privacy Bracket that allows regulatory space for a signatory country to provide data protection, but only if these safeguards are necessary and no less restrictive measure is available. The Privacy Bracket also permits each nation to decide for itself whether it wishes to permit personal data to be sent to a foreign country. In other words, the Bracketing defers to another day the creation of an international agreement about how privacy and trade are to be reconciled. The consequence is that each state has insisted on its own rules, which now vary widely across the world. These rules differ with respect to when and what personal data can be taken out of a country. Today, when truly global services are possible, and possible even for small enterprises, providing a global service becomes a huge challenge due to a complex regulatory thicket around international data transfers.

Internet lawyers are likely to be aware of the European Union's 'adequacy' requirement. This contribution from the EU has played a decisive role in developing the law of personal data transfers. The core EU idea is that of the necessity of a government power to stop data flows to nations without 'adequate' protection for the transferred personal information.[9] This concept has been adopted throughout the world, but without any uniform process or shared substantive definition of 'adequacy.' The result has been a splintering of the 'adequacy' principle. Countries define it in different ways and apply it according to their own policy agenda.

The EU's influential approach can be quickly sketched. Dating back to the EU Data Protection Directive (1998) and now enshrined in the GDPR (2018), the adequacy requirement permits transfers of per-

8 Rolf H. Weber and Dominic Staiger, *Transatlantic Data Protection in Practice* (Springer 2017).

9 Schwartz and Chander (n 5) 72.

sonal data to third countries only if these nations have an 'adequate' level of protection. The European Commission has the role of assessing whether this benchmark is met. According to the Court of Justice of the EU (CJEU), moreover, 'adequacy' of data protection requires a level that is 'essentially equivalent' between the EU and the country outside its borders. As the rainbow that leads to the pot of gold, an adequacy determination places a third country on equal footing with any EU member state for purposes of cross-border transfers. But the resulting EU list of adequate countries includes only ten nations outside of Europe of which two have only partial adequacy findings. These are Argentina (2003); Australia (2008), but only for Passenger Name Records; Canada (2001), but only for commercial organisations; Israel (2011); Japan (2019); New Zealand (2012); South Korea (2021); Switzerland (2000); the United Kingdom (2021); and Uruguay (2012).[10] In 2023, the European Commission restored the United States to this list, but again with a partial adequacy finding for commercial organisations participating in the EU-US Data Privacy Framework.

This paltry number of adequate countries is striking. Some 157 countries outside the EU now have data protection laws, but the EU has found only eight of these fully to have adequate protections in place. The EU process for adequacy determinations has failed to keep up with the rise of data protection laws and the importance of global data flows.

As a further difficulty, many non-EU nations have followed the adequacy approach. Our review of global privacy laws has revealed that 65 countries outside of the EU have data laws that permit or require adequacy reviews of foreign jurisdictions before allowing international transfers of personal data outside their borders.[11] The Privacy Bracket has encouraged many countries to adopt the adequacy approach.

The Bracketing led nations to search for mechanisms to safeguard the flow of personal information of their residents—a flow that increasingly occurs in a world of trade in digital services and goods. In theory, a finding of adequacy offers a trade-friendly solution to cross-border data flows, and one that is compatible with ensuring a high level of privacy protection. If the foreign country's privacy protections are essentially equivalent to one's own, transferring the personal data internationally is like transferring it domestically. But the results of the explosion in adequacy approaches have been inconsistent and idiosyncratic.

From Andora to Zimbabwe, there are now adequacy standards. These sometimes merely reference the term 'adequacy'; other statutes require a formal finding using this benchmark. There is no uniformity in these laws. Singapore demands a 'standard of protection of personal data ... comparable to the protection' under its domestic law. Quebec has a specific requirement for international transmission, and one that differs from other Canadian provinces. The Dubai International Financial Center (DIFC), a special economic zone in Dubai, has declared that California law is adequate. The DIFC has its own data protection law and an independent Office of the Commissioner of Data Protection. The finding of adequacy for California includes the possibility of 'similar relationships' being built with 'various US states' in the future.[12] In contrast, the European Union has not made a formal finding of adequacy, whether for the Golden State, any other jurisdiction in the United States, or for United States as a whole. Instead, it has negotiated the Data Privacy Framework, an opt-in process for American companies.

Moreover, the EU's own use of adequacy is far from unproblematic. As already noted, the EU has found only a handful of countries to be adequate. Moreover, the CJEU in two decisions, *Schrems I* and *Schrems II*, invalidated EU-US data sharing agreements, the precursors to the Data Privacy Framework, largely because of its concerns over US intelligence surveillance. At the same time, however, EU Member States have their own surveillance laws, as well as intelligence sharing arrangements with the United States. It is unclear whether EU residents have sufficient rights to challenge that surveillance, although the CJEU has insisted on strong protections for EU data subjects as regards US intelligence activities.

The regulatory thicket is further complicated by issues around consent. Obtaining consent before da-

10 'Adequacy decisions' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 24 September 2023.

11 Schwartz and Chander (n 5) 74.

12 'California Recognized By Dubai International Financial Centre Due to Data Protection Law and Regulations' (*CA.gov*, 9 August 2023) <https://cppa.ca.gov/announcements/2023/20230809.html > accessed 24 September 2023.

ta processing is an essential fair information practice, and one long enshrined as a basis for the legal processing of personal data. Yet, there are now differing parameters for the age of consent to data processing in the world's data privacy status. Even within the European Union, there is such a wide range. For example, the GDPR permits Member States to deviate from its basic rule of 16 years with an 'opening clause' that permits Member States to lower it anywhere from that age to 13.[13] Nine members of the EU have selected 13 years as the age of consent, six have chosen 14 years, three have opted for 15 years, and ten have remained with the GDPR's baseline of 16 years.[14] The result is a complicated maze for companies operating in the EU.

Outside of the EU, there is similar complexity. Japan has set the age of consent to personal data processing at 15 years old, China at 14, and California as under 13 years old. In California, however, there is a special requirement for children between the ages of 13 and 16. Generally, there is an *opt-out* in California privacy law for the sale of personal information. For children, however, there is an obligation on businesses to obtain an *opt-in* before sale of personal data.[15] If the child is under the age of 13 years old, a parent must affirmatively authorise the sale of information. Between 13 and 16 years of age, the teenager must affirmatively authorise the sale of the personal information.

The result is that obtaining consent from individuals is a tricky endeavour. Below the statutory age, parents must consent before a company can collect personal information from the minor. At the age of consent and above, the individual is able to agree to collection and use of their information, and, in some instances, such agreement must be obtained before data can be processed. Obtaining consent from users for companies operating in multiple jurisdictions cannot be resolved by simply adopting the strictest rule because no law meets this test across the board. Indeed, many laws deviate among issues such as the modalities of gaining consent and the requirements around information to be disclosed as part of obtaining consent.

In a world in which global trade is of central importance, the failure to resolve the conflict between privacy and trade has significant implications. At one time, the internet seemed to guarantee empowerment for all, including small companies in the world's poorest countries. The hope was for a democratisation of trade and a chance for a new global distribution of economic opportunities. The result of the current situation, however, favours the largest companies and organisations. These entities can manage the cost and complexities of international data privacy law.

A promising future now appears out of reach because of the regulatory thicket and splintering of adequacy. The harm has been to small and medium enterprises (SMEs), especially in less developed countries, and the benefit to big companies, especially those in the West. Indeed, large established tech companies begin with a significant global advantage due to their existing, extensive customer base. Through this existing relationship, and compared with companies starting from scratch, it has been easier for these enterprises to craft processes that comply with changing legal requirements while also maintaining data-rich relationships with current users. Through such connections, these companies have a major lead on any startup.

III. Possible Futures

We can imagine different futures for the privacy and trade relationship. Privacy and trade might wreck each other through conflict. Alternatively, privacy and trade might be reconciled to each other in ways that are mutually constitutive. Our imagined dateline is 1 January 2035.

Here is one possible headline for the *Wall Street Journal* on that day: 'Global Trade Collapses amid Privacy Fears.' The first paragraph reads as follows:

> Global trade fell to all-time lows this last year, the victim of economic stagnation and a complex of privacy and other laws that increasingly encumbered crossborder flows of data. Trade declined both in goods and services in 2034. Trade in commercial services reached a low not seen since 2009,

13 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) [2016] OJ L119/1.

14 Schwartz and Chander (n 5) 79.

15 'California Consumer Privacy Act (CCPA)' (*State of California – Department of Justice*, 10 May 2023) <https://oag.ca.gov/privacy/ccpa> accessed 24 September 2023.

> as financial and back office services declined due to growing restrictions on the flows of personal data across borders. Trade in goods fell as well, in part because of concerns that capabilities of digital goods and services might present risks for privacy and national security.

And here is an alternative future for 1 January 2035. The *Wall Street Journal*'s front page declares: 'Global Trade Reaches Record as Services Expand.' The first paragraph reads as follows:

> Increasing flows of goods and services across borders powered a record volume of trade in 2034. Services trade continued to grow at twice the rate of goods trade, as services companies increasingly globalize their supply chain. Both manufacturing and service sector enterprises increased the share of their workforce living outside the home country of the enterprise. Services growth was concentrated in the many nations that are party to the Council of Europe's Trade and Privacy Convention, which was ratified in 2030. Growth in services occurred across high, middle, and low-income countries. For many low-income or middle-income countries, revenues from outsourcing back-office services now account for more foreign exchange earnings than earned through remittances from workers abroad.

The question is how the world can reach something closer to the alternative future in which there is a record volume of trade. What would be the possible role in this better future of a global agreement that is both promotive of trade and of data privacy?

We begin by recognizing that privacy and trade have not in fact always been locked in a state of conflict. In fact, the desire to increase trade once led countries to strengthen privacy protections.[16] We can see this policy path within one of the European Union's landmark privacy laws, namely the Data Protection Directive (1995). The official title of this instrument explicitly embraces trade as a key goal: 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.'[17] The Directive offered an elegant solution to the possible trade and privacy conflict—if the foreign state agreed to a core set of protections, then claims of the unsuitability of a foreign state to receive personal data could not stop data flows. The idea was that of adequacy approach, which, at that point in time, had not yet been widely adopted outside of Europe and had not yet been fragmented in its substance. That was also the solution that the European Union turned to when it sought to create a single market within its Member States by requiring them to harmonise their own data protection laws.

This approach in international privacy law contrasted with the Privacy Bracket approach adopted by trade law that we described earlier. Trade law, unable to come to an agreement on a core set of privacy protections, simply allowed each state to insist on its own privacy rules, as long as they were necessary to achieve privacy protections and did not constitute arbitrary or unjustifiable discrimination.

The World Trade Organization is now revisiting its rules with respect to cross-border data flows through a Joint Statement Initiative for Electronic Commerce.[18] Any such agreement will cover only the states that agree to sign on, thus making this a plurilateral arrangement. Some 87 WTO members are participating in the negotiations. Unfortunately, the regulatory positions of some of the major negotiating partners suggest that the negotiators are likely far apart on issues related to data flows.

The European Union is seeking to ensure that its decisions related to data protection are not subject to second guessing through a trade tribunal. In its latest bilateral trade agreements, the EU seeks to exclude measures and decisions taken under the banner of data protection from review under the trade dispute settlement mechanism.[19] At the same time, China has established strict cybersecurity measures that would require pre-approval for the transfer of personal information out of that country when the transmission is deemed to raise national security risks.[20] As for the United States, it would prefer to have stronger protections for data flows. Its goal is to ensure that privacy measures that are unjustified

16 Anupam Chander, 'The Trade Origins of Privacy Law' (2023) Indiana Law Journal (forthcoming).

17 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/1.

18 WTO, *Joint Statement on Electronic Commerce* (25 January 2019) WT/L/1056.

19 Mira Burri, 'The Impact of Digitalization on Global Trade Law' (2023) 24 German Law Journal 551, 569.

20 Anupam Chander and Haochen Sun, 'Sovereignty 2.0' (2022) 55 Vanderbilt Journal of Transnational Law 283, 296.

or discriminatory can be sanctioned within the trade dispute settlement system.[21]

Hence, there is no agreement at present regarding the Joint Statement Initiative for Electronic Commerce. But there is growing consensus about an overarching principle—'data free flows with trust,' or DFFT. Proposed originally by Prime Minister Shinzo Abe at the World Economic Forum meeting in 2019 and adopted as a declaration by the G20 that year, DFFT seeks to ensure the free flow of data while ensuring privacy, security, and intellectual property.[22] DFFT hopes

> to reconcile two related and compatible policy objectives: (1) promoting free data flows to foster economic growth and (2) protecting individual privacy, national security, and IP through trusted regulations.[23]

The Japanese government has established a research centre at the Economic Research Institute for ASEAN and East Asia in Jakarta, Indonesia, to promote trusted cross-border data flows.[24]

There are two principal obstacles to a broad agreement that embraces DFFT. First, reaching an agreement on a baseline set of privacy rules will prove challenging. The WTO is not the ideal forum in which to fashion the privacy rules themselves. Rather, the WTO often turns to standards adopted by a widely-respected international forum, and requires nations to justify deviation. There are a variety of possible fora for reaching such a substantive agreement, including the Global Privacy Assembly, which is constituted by data protection commissioners from around the world.

Some will be sceptical about the possibility of a broad privacy agreement. The world's data privacy laws may seem too diverse and far apart for any general agreement. With the California Consumer Privacy Act and its California Consumer Protection Agency, the Golden State now has the strongest data privacy laws in the United States, and a regime that shares some of the most important elements of European data protection law. But California's privacy laws differ from those of the European Union, not to mention from the privacy laws of China and India.[25]

At the same time, there is a significant core of convergence between the various frameworks that might offer a starting point upon which to build.[26] As the OECD explained in its Digital Economy Paper, there are now 'important complementarities between existing instruments' and 'evidence of convergence towards common principles on privacy ... as well as towards common language and binding commitments in the context of trade.'[27] A global agreement could build on the areas of overlap between the various regimes, and then seek to resolve the differences.

Alternatively, the Council of Europe's Convention 108 and its successor Convention 108+ could offer an alternative starting point to achieve an international agreement facilitating DFFT.[28] Yet another approach to establishing the substantive privacy norms for DFFT would be to begin with the EU-US Data Privacy Framework, which represents an effort to meet EU standards on terms that the United States can both satisfy and abide.[29]

If a broad international solution proves impossible, companies will turn to less comprehensive solutions in alternative mechanisms that lean heavily on corporate compliance—such as standard contractual clauses, certification mechanisms, or codes of conduct. Such transmissions systems permit cross-border data transfer through commitments that are

---

21 Rachel F. Fefer, 'Data Flows, Online Privacy, and Trade Policy' (*Congressional Research Service*, 26 March 2020) <https://crsreports.congress.gov/product/pdf/R/R45584> accessed 24 September 2023

22 Aidan Arasasingham and Matthew P. Goodman, 'Operationalizing Data Free Flow with Trust (DFFT)' (*Center for Strategic and International Studies*, 13 April 2023) <https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft> accessed 17 September 2023.

23 Ibid.

24 Shiko Ueda, 'Japan, ASEAN to create entity for supporting free flow of data' (*Nikkei Asia*, 3 July 2023) <https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/Japan-ASEAN-to-create-entity-for-supporting-free-flow-of-data> accessed 17 September 2023.

25 Anupam Chander, Margot Kaminski, and William McGeveran, 'Catalyzing Privacy Law' (2021) 105 Minnesota Law Review 1733, 1746.

26 Pascal Lamy and others, 'Global Governance for the Digital Ecosystems' (*Centre on Regulation in Europe*, 11 November 2022) <https://cerre.eu/wp-content/uploads/2022/11/GGDE_FullReport.pdf> accessed 17 September 2023.

27 'Fostering Cross-Border Data Flows With Trust' (*OECD Digital Economy Papers*, December 2022) <https://rb.gy/tftrk> accessed 26 September 2023.

28 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series – No. 108, Strasbourg: Council of Europe, 28 January 1981, CETS 108; 'Convention 108+' (*Council of Europe*, June 2018) <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 26 September 2023.

29 'EU-U.S. Data Privacy Framework Principles Issued by the U.S. Department of Commerce' (*Data Privacy Framework Program*, 2023) <https://rb.gy/3x6dq> accessed 26 September 2023; Commission, 'Regulation on the adequate level of protection of personal data under the EU-US Data Privacy Framework (Commission Implementing Decision) (2023).

backed up through both public and private enforcement. The Global Cross-Border Privacy Rules (CBPR) adopt such an accountability-based approach. Building on the Asian Pacific Economic Cooperation, the Global CBPR Forum currently has the Member countries: Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, Chinese Taipei, and the United States of America.[30]

The second major challenge to a broad agreement will be issues related to national security. Governments are increasingly concerned that allowing their citizens' personal data to flow out from their national borders might bring it into the hands of foreign surveillance. These transmissions might jeopardise the privacy of the data subjects and the national security of the country. As for national security, countries may fear that allowing data to flow from their national borders will allowing foreign countries access to personal data that might compromise their national security by revealing secrets or allowing blackmail.

National security, then, might seem an impassable roadblock to trade in data. There has, however, been significant developments that point to an emerging framework for reciprocity. To begin with, the EU and the United States have agreed upon a new arrangement, the Data Privacy Framework, that will better protect EU personal data transferred to the United States.[31] The Biden Administration has backed up this agreement with Executive Order 14086, which creates a Data Protection Review Court within the US Department of Justice.[32] This new court will adjudicate complaints from foreign 'qualifying states' about US collection of signals intelligence. The United States has formerly designated the European Union as well as the nations in the European Economic Area as qualifying under this Executive Order. This move to reciprocity is based on an evaluation of whether the foreign jurisdiction provides safeguards for US persons data collected by its own intelligence services; allows transfers of personal data for commercial purposes to the United States; and the national interests of the United States support this designation.

The United States has also entered into executive agreements for sharing data under the CLOUD Act.[33] This statute amended the Stored Communications Act (SCA), part of the Electronic Communications Privacy Act, to clarify that providers had to follow their obligations under the SCA regardless of where that information is located. This statue also authorised the US government to enter into executive agreements with foreign governments for reciprocal access to electronic information held by providers in their respective nations. The United States has now entered into such agreements with the United Kingdom and Australia, and is negotiating agreements with Canada and the European Union.[34]

Finally, in 2022, the OECD countries agreed on an OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, demonstrating that countries were willing to commit to rules for government access to personal data.[35] Kenneth Propp has pointed to the OECD Declaration as representing 'a notable degree of multilateral consensus on government surveillance safeguards.'[36] He also notes that the US Department of Justice explicitly relied on the Declaration in its recent memorandum finding that the European Union and European Economic Area qualified for reciprocity under Executive Order 14086. All of these steps suggest significant progress regarding global rules for government access to personal data, including redress mechanisms when those rules are breached.

IV. Conclusion

A major issue in data protection law over the next decade will be how it interacts with trade law. The current conflict between these two areas has the potential to lead to economic stagnation due to increas-

30 'About CBPRs' (*Cross Border Privacy Rules System*) <https://cbprs.org/about-cbprs/> accessed 26 September 2023.

31 'Data Privacy Framework (DPF) Overview' (*Data Privacy Framework Program*) <https://www.dataprivacyframework.gov/s/program-overview> accessed 26 September 2023.

32 'Executive Order 14086 – Policy and Procedures' (*US Department of State*, 3 July 2023) <https://rb.gy/hcmui> accessed 26 September 2023.

33 Paul M. Schwartz, 'Legal Access to the Global Cloud' (2018) 118 Columbia Law Review 1681, 1752.

34 'Cloud Act Resources' (*United States Department of Justice*) <https://www.justice.gov/criminal-oia/cloud-act-resources> accessed 17 September 2023.

35 'Declaration on Government Access to Personal Data Held by Private Sector Employees' (*OECD Legal Instruments*, 13 December 2022) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487> accessed 26 September 2023.

36 Kenneth Propp, 'Revenge, or Reciprocity? The U.S.'s Review of Europe's SIGINT Safeguards' (*Lawfare*, 29 August 2023) <https://www.lawfaremedia.org/article/revenge-or-reciprocity-the-u.s.-s-review-of-europe-s-sigint-safeguards> accessed 17 September 2023.

ingly cumbersome restrictions on cross-border flows of data. One reason for these potential difficulties would be the ongoing splintering of rules around the adequacy requirement for international data transfers. Fortunately, there are now signs of convergence between different existing frameworks for 'data free flows with trust' (DFFT). Recall that the Privacy Bracket in GATS prevents countries from blocking trade with providers in countries where 'like conditions prevail.' The goal of international privacy policymakers should be to work towards such international harmonisation of their standards. To reach this goal, a global agreement is needed to reach agreement on baseline privacy rules. Such an agreement will need to draw on various institutions beyond those responsible for data privacy policymaking in the European Union and United States, including the Global Privacy Assembly, WTO, and OECD.