9-2023

A Trusted Framework for Cross-Border Data Flows

Alex Joel
American University Washington College of Law, ajoel@wcl.american.edu

G | M | F

IDEAS LEADERSHIP HOPE

Report

A Trusted Framework for Cross-Border Data Flows

Tech, Law and Security Program,
American University Washington College of Law
and the German Marshall Fund of the United States

September 2023

Preface

The German Marshall Fund of the United States (GMF), in cooperation with the Tech, Law and Security Program (TLS) of the American University Washington College of Law, and with support from Microsoft, convened a Global Taskforce to Promote Trusted Sharing of Data comprising experts from civil society, academia, and industry to submit proposals for harmonizing approaches to global data use and sharing. Former US Ambassador to the Organisation for Economic Co-operation and Development (OECD) and GMF Distinguished Fellow Karen Kornbluh and Microsoft Chief Privacy Officer and Corporate Vice President Julie Brill co-chaired the taskforce; TLS Senior Project Director Alex Joel provided subject matter expertise. The taskforce's goal was to explore the common elements of existing proposals and identify viable paths toward a harmonized regime that allows data to flow in a trusted, secure, and rights-protecting way.

This paper reflects the views of its authors at TLS and GMF. It was prepared by TLS's Alex Joel with the assistance of Shanzay Pervaiz, who conducted extensive research and engaged with a range of experts, policymakers, and practitioners on whose professional experience and expertise this paper draws. GMF's Karen Kornbluh and Julia Trehu also provided expert input.

Over 14 months, GMF and TLS jointly convened a series of roundtable discussions among members of the independent global taskforce. Its discussions did not seek to achieve agreement or consensus. Rather, members expressed a wide range of opinions and perspectives that greatly benefited this paper, which does not necessarily reflect the views of taskforce members (individually or collectively). Taskforce participation does not imply endorsement of or agreement with this paper in whole or in part.

GMF and TLS thank the participants for selflessly sharing their time, expertise, and insights, and for engaging in productive and positive discussions on challenging issues. This paper was originally posted by GMF on their website.

See Annex A for a list of participants.

Table of Contents

Introduction

The goal of this paper is to identify concrete and practicable measures that enable beneficial cross-border data flows to continue while guarding against the risks such flows can pose. These measures must address the reasons governments seek to restrict data flows by giving them confidence that, when private-sector entities transfer data across borders, (1) those entities will protect individuals' privacy (commercial privacy); and (2) the recipient[1] country's government will also protect privacy when it seeks access to that data (trusted government access). The topics of commercial privacy and trusted government access are inextricably interlinked, and both must be addressed to achieve trust.

Note: For the sake of simplicity, this paper focuses on two important areas in which rapid progress seems readily achievable: commercial privacy and trusted government access. This paper does not address nonpersonal data or other areas that could involve data flow restrictions. A framework for trusted data flows in commercial privacy and trusted government access will spur progress in other areas and will help distinguish between data flow restrictions that, as stated in the G7's Hiroshima Leaders' Communiqué of May 20, 2023, raise "unjustified obstacles" and those that are "implemented to achieve the legitimate public policy interests of each country."

To be effective, a trusted framework for cross-border data flows must be **open to democracies operating under the rule of law**, and must be **rights-protective**, **practicable**, and **scalable.** The framework must provide meaningful privacy safeguards that are enforced through effective accountability mechanisms. Those protections must be achievable by democracies that respect the rule of law even if they may need to make improvements in certain areas. The framework must also be scalable to keep up with the rapid and global pace of change, and enable efficient and objective decision-making.

This paper outlines such a framework, building on progress made in multilateral efforts. Stakeholders should quickly initiate a multilateral, transparent process that leverages this progress and that focuses on the areas of commercial privacy and trusted government access.

[1] When data flows across borders, the country in which data originates is called, in this paper, the "originating country." The country to which data flows is referred to as the "recipient country." Some have used the term "export" to describe cross-border data flows. Using that metaphor, the originating country would be the data "exporter" and the recipient country would be the "importer."

Background

As the world becomes increasingly interconnected through technology, political leaders are recognizing "the importance of secure and resilient digital infrastructure as the foundation of society and the economy."[2] For private-sector entities, cross-border data flows "[underpin] daily business operations, logistics, supply chains and international communication."[3] Responsible cross-border data flows can also promote human rights,[4] cybersecurity,[5] economic development,[6] financial inclusion, health, sustainability, and other legitimate government objectives.[7] At the same time, it is important to recognize the legitimate reasons government entities have for seeking access to such data, such as to protect national security and public safety. As some have noted, "responsible use of data enables economic growth and brings benefits and progress to people, governments, and societies at large."[8] On the other hand, such data flows can raise risks to countries and individuals.[9] Unless those risks are addressed, the benefits of cross-border data flows are themselves at risk.[10]

---

[2] The Office of the Privacy Commissioner of Canada, Communiqué: G7 Data Protection and Privacy Authorities, (June 21, 2023). https://www.priv.gc.ca/en/opc-news/speeches/2023/communique-g7-230621
This recognition is particularly evident among industrialized countries such as those in the G7. While this issue is also important for countries in the Global South, they also face other pressing challenges. See, e.g., Organisation for Economic Co-operation and Development (OECD), Development Co-operation Report 2023, Chapter 18 (responding to Global South views on development priorities, progress and partner performance). https://www.oecd-ilibrary.org/sites/265af16b-en/index.html?itemId=/content/component/265af16b-en

[3] OECD, Data governance. https://www.oecd.org/digital/data-governance/#:~:text=Cross%2Dborder%20data%20flows%20are,supply%20chains%20and%20international%20communication

[4] "Digital technology already delivers many benefits. Its value for human rights and development is enormous. We can connect and communicate around the globe as never before. We can empower, inform and investigate. We can use encrypted communications, satellite imagery and data streams to directly defend and promote human rights," Michele Bachelet, UN High Commissioner for Human Rights, Human rights in the digital age – Can they make a difference?, Keynote speech, Japan Society, New York, October 27, 2019. https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age

[5] See, e.g., Peter Swire and DeBrae Kennedy-Mayo, The Effects of Data Localization on Cybersecurity - Organizational Effects, Georgia Tech Scheller College of Business, June 15, 2023. https://ssrn.com/abstract=4030905 or http://dx.doi.org/10.2139/ssrn.4030905

[6] World Bank, World Development Report — Data For Better Lives (2021). https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf

[7] Global Data Alliance, Issues, 2023. https://globaldataalliance.org/issues/; Global Data Alliance, Sectors, 2023. https://globaldataalliance.org/sectors/

[8] Centre for Information Policy Leadership (CIPL), The "Real Life Harms" of Data Localization Policies, March 2023. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf

[9] "Cross-border data flows are also seen to amplify challenges such as to privacy and data protection, intellectual property protection, digital security, national security, regulatory reach, trade, competition, and industrial policy." OECD, supra note 3. See also Peter Swire and DeBrae Kennedy-Mayo, The Effects of Data Localization on Cybersecurity - Organizational Effects, Georgia Tech Scheller College of Business, June 15, 2023. https://ssrn.com/abstract=4030905 or http://dx.doi.org/10.2139/ssrn.4030905

[10] "Data flows with trust are critical, not only for a free and open internet but also for the realisation of human rights online. But without robust and comprehensive data protection, data security, privacy safeguards, and

Since the 1980s, several global instruments have been created to uphold the interoperability of personal data. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines) is one of the first significant global data protection initiatives.[11] These guidelines adopted many of the Fair Information Practice Principles[12] and reflected a commitment to "promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information."[13] Convention 108, established in 1981 as the first legally binding international instrument in the data protection field, is another important initiative. Convention 108[14] requires its parties to adopt domestic legislation that incorporates its principles,[15] which include purpose limitation, data subject rights, and controller and processor obligations.[16] Then, in 1995, the EU adopted the European Data Protection Directive[17], which the bloc replaced in 2018 with the General Data Protection Regulation (GDPR)[18]. Since the passage of these seminal instruments, many countries have enacted legislation[19] and developed tools and frameworks using similar principles to bolster the trusted free flow of data while providing safeguards to protect individual rights and liberties.

---

human rights frameworks that protect people's information, none of these benefits can be achieved." Estelle Masse, Speech delivered by Estelle Massé, Europe Legislative Manager and Global Data Protection Lead at Access Now, G7-DPA Roundtable in Bonn, Sept. 6, 2022. https://www.accessnow.org/wp-content/uploads/2022/09/Estelle-Masse-G7-speech-6-Sept-2022.pdf

[11] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Legal Instruments, Sept. 22, 1980. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[12] In 1973, the Department of Health, Education, and Welfare Advisory Committee released a report, Records, Computers and the Rights of Citizens, that articulated the Fair Information Practice Principles (FIPPs). The FIPPs are a framework used for determining responsible data protection practices as private and public sectors were obtaining an increasing amount of personal data.

[13] U.S. Department of Health, Education & Welfare, Records, Computers and the Rights of Citizens, Department of Justice, July 1973. https://www.justice.gov/opcl/docs/rec-com-rights.pdf

[14] Convention 108 was amended in 2018 and is now referred to as Convention 108+.

[15] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Ch. II, Article 4, Council of Europe European Treaty - No. 108, Jan. 28, 1981. https://rm.coe.int/1680078b37

[16] Ibid., Articles 5-8.

[17] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046
For more information on the background of the Data Protection Directive, see Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, Sept. 14, 2015. https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf

[18] 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). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1692462532043

[19] International Association of Privacy Professionals (IAPP), Global Comprehensive Privacy Law Mapping Chart, April 2022. https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf; Convention of Cybercrime, Nov. 23, 2011, ETS No. 185. https://rm.coe.int/1680081561

At the same, some countries are adopting legal approaches that condition, restrict, or, in some cases, prohibit cross-border data flows.[20] Originating countries seek to control cross-border data flows for several reasons. One is ensuring that privacy rights that the country has granted its citizens or residents will not be compromised when their data is transferred internationally. Other rationales include facilitating domestic law enforcement access and exercising greater control over information developed domestically.[21] These concerns are legitimate, but the resulting policies can disrupt industries, digital landscapes, and global communications.[22] These measures may also not achieve their intended effect.[23] The resulting global picture is characterized by fragmented regulation and a need for bilateral national arrangements.

Without concerted efforts by all stakeholders, current measures for facilitating cross-border data flows could become increasingly difficult to implement in a manner that protects individual rights and enables countries to derive important economic and societal benefits from data flows. The G7's recent Data Free Flow with Trust (DFFT)[24] initiative is an important effort to harmonize splintered approaches to cross-border data flows. To operationalize DFFT, G7 digital and technology ministers published a declaration that stated their commitment to "advance international policy discussions to harness the full potential of cross-border data

[20] Some countries seek to achieve greater control through "hard" data localization measures. Other countries allow for data flows to take place if they are satisfied that data will be processed in ways that meet their legal requirements for protecting privacy. For example, many countries have comprehensive privacy laws with provisions that potentially restrict cross-border data transfers. IAPP, Global Comprehensive Privacy Law Mapping Chart, April 2022. https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf Some of these privacy laws implement adequacy models, in which the originating country determines whether a third country meets its "data privacy standards" for cross-border data transfers. Joe Jones, Infographic: Global adequacy capabilities, IAPP, April 2023. https://iapp.org/resources/article/infographic-global-adequacy-capabilities/

[21] Anupam Chander and Uyên P. Lê, Data Nationalism, 64 Emory L. J. 677, 714, 2015. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/

[22] Centre for Information Policy Leadership (CIPL), The "Real Life Harms" of Data Localization Policies, March 2023. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf; Iverna McGowan and Greg Nojeim, Joint Statement Calls Out Internet Fragmentation, Center for Democracy & Technology, Sept. 22, 2021. https://cdt.org/insights/joint-statement-calls-out-internet-fragmentation/; See also Theodore Christakis, 'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy, Dec. 7, 2020. https://ssrn.com/abstract=3748098

[23] See Shanzay Pervaiz and Alex Joel, Data Localization and Government Access to Data Stored Abroad: Discussion Paper 2, Tech, Law & Security Program at American University Washington College of Law, March 30, 2023. https://digitalcommons.wcl.american.edu/research/87/

[24] World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, May 2020. https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

flows" through an Institutional Arrangement for Partnership (IAP). [25] The IAP will work to address several issues areas including data localization, regulatory cooperation, trusted government access to data, and data sharing.[26] Further, the G7 Data Protection and Privacy Authorities Roundtable affirmed their support for current international frameworks and for operationalizing DFFT.[27] The framework presented in this paper advances DFFT and IAP goals by using several building blocks listed below.

A Trust-based Framework for Data Flows

Countries must replace the current fragmented approach with a common framework for ensuring international data flows in a rights-protective manner. Such a framework must be open to **democracies governed by the rule of law**. The framework must also be **rights-protective,[28] practicable, and scalable**.

Key Elements

Rule of Law

The foundation of a trust-based framework for cross-border data flows is that participating countries must share a demonstrable commitment to democratic governance under the rule of law. With that foundation, countries can have confidence that legal obligations to protect rights will be respected and enforced. A democracy governed by rule of law ensures "political rights, civil liberties, and mechanisms of accountability which in turn affirm the political equality of all citizens and constrain potential abuses of state power."[29] In authoritarian regimes, "power is concentrated in the hands of a single leader or small elite", and the regime governs without

[25] G7, Ministerial Declaration, G7 Digital and Tech Ministers' Meeting, April 30, 2023. http://www.g7.utoronto.ca/ict/2023-ministerial_declaration_dtmm.pdf

[26] G7, G7 Digital and Tech Track Annex 1, April 30, 2023. http://www.g7.utoronto.ca/ict/2023-annex1.pdf

[27] The Office of the Privacy Commissioner of Canada, supra note 2.

[28] The term "rights-protective" is intended to connote the need for a trust-based framework to protect privacy and other fundamental rights. In related contexts, some use the term "rights-based", which has a similar connotation. See, e.g., European Commission, The Human Rights Based Approach. https://wikis.ec.europa.eu/pages/viewpage.action?pageId=50108948 ("By applying these principles, the HRBA identifies states and their institutions as duty-bearers that are accountable for respecting, protecting and fulfilling human rights.")

[29] Guillermo O'Donnell, The Quality of Democracy: Why the Rule of Law Matters, Journal of Democracy, Vol. 15, No. 4, 32 (2004).

consent of its citizens.[30] Under authoritarianism, there are no legitimate accountability mechanisms, and transfer of executive power does not exist.[31]

Countries seeking to benefit from the framework should meet internationally recognized criteria for democratic governance under the rule of law.[32] If a recipient country does not meet those criteria, then originating countries may well need to follow individualized approaches to restrict data flows and ensure rights are protected.

Rights-Protective

Democracies governed by the rule of law uphold individual rights and seek to ensure that the rights it grants its citizens or residents are not compromised in international data flows. A framework for such data flows must consequently include **meaningful safeguards** that effectuate individual rights and protect data from the risk of abuse and misuse by private-sector entities and governments. These safeguards include protecting against access that is inconsistent with democratic values and the rule of law, or that is unconstrained, unreasonable, arbitrary, or disproportionate. A rights-protective framework must also have in place **accountability mechanisms** to ensure that those processing data are properly implementing safeguards (including internal and external oversight and individual redress). In short, the framework must provide assurance that processing entities (whether government or the private sector) respect individuals' privacy and other fundamental rights in the recipient country in a manner that is comparable (albeit not identical) to practices in the originating country.[33]

Practicable

The framework must consider that countries have different legal systems and that each, therefore, may establish its own safeguards and accountability mechanisms. Recipient countries should not be expected to fundamentally alter their legal frameworks to duplicate an originating country's laws or simply accept those another country already has in place. At the

---

[30] Natasha Lindstaedt, Authoritarianism, Encyclopedia Britannica, June 2023. https://www.britannica.com/topic/authoritarianism

[31] Ibid.

[32] See United Nations, What is the Rule of Law. https://www.un.org/ruleoflaw/what-is-the-rule-of-law/; Summit for Democracy, Joint Statement And Call To Action On The Rule Of Law And People-Centered Justice: Renewing A Core Pillar Of Democracy, USAID. https://www.usaid.gov/sites/default/files/2023-04/Joint-Statement-Call-to-Action-on-the-Rule-of-Law-and-PCJ-April-14-2023.pdf; Venice Commission of the Council of Europe, The Rule Of Law Checklist, March 2016. https://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule_of_Law_Check_List.pdf

[33] Note that this assurance depends on the degree to which the recipient country is a democracy operating under the rule of law.

same time, a country may not rest on its laurels for being a democracy governed by the rule of law. It must fill any legal and procedural gaps or improve any deficiencies to provide meaningful safeguards and effective accountability mechanisms.[34]

Scalable

The framework must keep pace with the speed, scale, and global reach of international data flows, and it must enable fair and efficient cross-border data-flow determinations based on agreed, objective criteria.

The **building blocks** for such a framework already exist. They include:

- work done on cross-border transfer mechanisms under the GDPR[35] and comparable laws outside the EU
- the EU-US Data Privacy Framework[36]
- OECD Privacy Guidelines[37]
- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework[38] and the Global Cross-Border Privacy Rules (CBPR)[39]
- the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities (OECD TGA Declaration) [40]
- the Global Privacy Assembly's 2021 resolution on government access to data[41]

---

[34] Christopher Docksey, Keynote on Accountability At the 41st Conference of Data Protection and Privacy Commissioners in Tirana, Albania, Oct. 31, 2019. https://informationaccountability.org/2019/10/christopher-docksey-keynote-on-accountability-at-the-41st-conference-of-data-protection-and-privacy-commissioners-24-october-2019-in-tirana-albania/; See also Christopher Docksey, Article 24 in C. Kuner, L. A. Bygrave, and C. Docksey (eds.), The EU General Data Protection Regulation: A Commentary, OUP, 2020, pp. 555–570.

[35]GDPR, supra note 19. In November 2021 the Court of Justice of the European Union published a fact sheet on the protection of personal data. https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf

[36] European Commission, Adequacy decision for the EU-US Data Privacy Framework, July 10, 2023. https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

[37] OECD, OECD Privacy Guidelines, Sept. 22, 1980. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

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

[39] US Department of Commerce, Global Cross-Border Privacy Rules Declaration, 2022. https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[40] OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, Dec. 13, 2022. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

[41] Global Privacy Assembly, Adopted resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes, Oct. 2021. https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted.pdf

- Council of Europe Convention 108+[42]

A Framework for Commercial Privacy

The cross-border issues on commercial privacy have been much discussed, and the building blocks for a rights-protective framework are well known. The challenge now is determining the best way to use the building blocks to reach agreement on a common set of practicable and scalable safeguards and accountability measures.

The EU has led on data protection through GDPR, and many countries are using GDPR as a model for their own data protection laws.[43] Such laws focus on transfer mechanisms based to a significant degree on individual, country-by-country determinations. The European Commission has been working to review countries for adequacy, finalizing its findings in recent years for South Korea, the United Kingdom, and the United States. There are now 16 countries with adequacy findings, though many of those predate recent Court of Justice of the European Union (CJEU) rulings and are being re-examined[44] given recently articulated standards for national security access to data.[45] The EU has also issued guidance on other transfer mechanisms.[46] Work is being done to identify commonalities and differences in standard

---

[42] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. https://rm.coe.int/1680078b37; Information about additional protocols and amendments on Convention 108+ can be found at https://www.coe.int/en/web/data-protection/convention108-and-protocol.

[43] Joe Jones, supra note 13. See also Christopher Kuner, The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards, National Law Review of India, Nov. 20, 2021. https://ssrn.com/abstract=3964672

[44] Joe Jones, LinkedIn post, July 2023 (summarizing his July 21, 2023, interview with Bruno Gencarelli, acting director of Fundamental Rights and Rule of Law, DG Justice and Consumer Affairs, European Commission). https://www.linkedin.com/posts/joe-jones-b1793bb6_privacypros-privacy-dataprivacyframework-activity-7087818429327384576-ohui/; Note the GDPR calls for periodic reviews of adequacy decision. See Article 45, ¶3-6 and Article 97(2)(a).

[45] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, joined party: Rights Ireland Ltd., 2015. https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143358; Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Maximillian Schrems, 2020. https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155

[46] European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, Jan. 14, 2021. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en; EDPB, Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), Jan. 2022. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_en; European Commission, Binding Corporate Rules (BCR), https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-

contractual clauses.[47] The APEC Privacy Framework also provides a model for cross-border transfers through CBPR, and several countries[48] recently established the Global CBPR Forum to "promote interoperability and help bridge different regulatory approaches to data protection and privacy." And countries such as India have enacted privacy laws that permit cross-border data transfers except in cases where the government restricts the transfer.[49]

Separate processes under the GDPR and CBPR frameworks are underway to address cross-border data flow issues. These approaches share common goals, and their core privacy principles spring from a common foundation. Nonetheless, key differences to be bridged remain.[50] The G7 has called for countries "to work towards identifying commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, in order to foster future interoperability such as through supporting multi-stakeholder engagement, leveraging the role of technologies, and clarifying domestic and municipal policies and due processes."[51] It is important for this work to be based on the aforementioned principles, focusing on measures that within democracies under the rule of law are rights-protective (meaningful safeguards and effective accountability mechanisms), practicable (achievable by rule-of-law democracies), and scalable (efficient and fair determinations).

Going forward, stakeholders should seek agreement on:

---

bcr_en#:~:text=Relevant%20documents-,What%20are%20binding%20corporate%20rules%3F,group%20of%20undertakings%20or%20enterprises; EDPB, Guidelines 07/2022 on certification as a tool for transfers, July 2022. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_ga

[47] Lee Matheson, NOT-SO-STANDARD CLAUSES – Examining Three Regional Contractual Frameworks for International Data Transfers, The Future of Privacy Forum, March 2023. https://fpf.org/wp-content/uploads/2023/03/FPF-SCC-Not-So-Standard-Clauses-Report-FINAL-single-pages-1.pdf; IAPP, A practical comparison of the EU, China and ASEAN standard contractual clauses, June 2023. https://iapp.org/resources/article/a-practical-comparison-of-the-eu-china-and-asean-standard-contractual-clauses/#sccs

[48] This includes Canada, Japan, the Philippines, Singapore, South Korea, Taiwan, and the United States.

[49] India Digital Personal Data Protection Act of 2023, Art. 16(2). https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf

[50] See, e.g., Article 29 Data Protection Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, Feb. 27, 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf; Alex Wall, GDPR matchup: The APEC Privacy Framework and Cross-Border Privacy Rules, IAPP, May 31, 2017. https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/; L. Robinson, K. Kizawa, and E. Ronchi, Interoperability of privacy and data protection frameworks, OECD Going Digital Toolkit Note, No. 21, 2021. https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

[51] G7 Hiroshima Leaders' Communiqué, ¶39, May 20, 2023. https://www.g7hiroshima.go.jp/documents/pdf/Leaders_Communique_01_en.pdf

- **a common benchmark** for identifying democracies that respect the rule of law

- **a core set of rights-protective principles** comprising privacy safeguards drawn from key commonalities among well-established instruments such as GDPR, the OECD Privacy Guidelines, and the APEC Privacy Framework,[52] and from accountability mechanisms enforceable through contractual commitments, effective regulatory oversight, and individual redress, and reinforced by formalized means for international regulatory and enforcement cooperation

- **practicability** by acknowledging that a range of ways exists for democracies that respect the rule of law to protect rights while enabling stakeholders to understand and address specific areas in need of improvement

- **scalability** through use of a "certification" or similar mechanism that enables governments and private-sector entities to publicly commit themselves to adhering transparently and accountably to an international data flow framework while enabling objective assessments and efficient decision-making[53]

Given the amount of time, expertise, and resources devoted to the topic of commercial privacy in recent years, progress is readily achievable if stakeholders commit to seeking agreement. As for the linkage between commercial privacy issues and concerns about government access to data, those are addressed below.

Trusted Government Access

Concerns about government access to data arise in two distinct but interrelated contexts. First, will the recipient country's government appropriately protect privacy when it seeks access to that data for national security or law enforcement purposes? Second, will the originating country's law enforcement agencies be able to obtain lawful access to data "exported" to the recipient country?

[52] Ibid. Although these instruments vary in a range of ways, including in the degree to which they impose binding obligations, stakeholders can nonetheless "work towards identifying commonalities, complementarities and elements of convergence."

[53] It is important to keep in mind the ongoing work on contractual clauses, as highlighted by the Roundtable of G7 Data Protection and Privacy Authorities, supra note 2, ¶9.

A framework for trust-based data flows must prioritize these concerns. Progress is achievable if stakeholders recognize the importance of the following:

- **Ensuring governments are committed to the process**. Only governments, working together, can resolve the issues at hand. Private-sector entities, on their own, are much less able to adopt measures to provide safeguards and accountability because they must comply with lawful government-access demands and cannot contract their way out of them. Relevant government bodies must commit to participating proactively and constructively in finding ways that allow for safeguards and appropriate government access, and they must accept the potential need to resolve conflicts, amend laws, or improve deficiencies during that process.

- **Enhancing mutual understanding across sectors and borders.** Progress is possible only when stakeholders understand each other's perspectives well. There are several dimensions to this challenge. First, laws, policies, and practices in the commercial privacy arena differ substantially from those governing national security and law enforcement access. Approaches that might work in commercial privacy, for example, may not align neatly with how countries' legal systems regulate national security and law enforcement activities.[54] Second, despite recent progress in national security transparency, more headway is needed to enhance understanding of this complex and secretive issue. Third, although democracies share certain principles for law enforcement and national security access to data, there are significant differences in how those principles manifest themselves in a country's legal framework. Any attempt to enhance understanding among stakeholders must address these dimensions and be inclusive. Efforts to flesh out the framework for trusted government access, for example, must embrace government officials, the private sector, and civil society. Agencies responsible for carrying out or overseeing national security and law enforcement activities must also be involved, as must government entities responsible for administering and enforcing privacy and data protection requirements.

- **Following up on progress on cross-border law enforcement access.** Stakeholders can build on structures, processes, and commitments related to law enforcement access to data. Governments have already done important work in developing approaches that enable such cross-border access to data while simultaneously protecting privacy and other rights. A wide range of countries, for example, have ratified the Budapest Cybercrime Convention and now have years of experience implementing its provisions.

[54] For example, a company cannot make contractual commitments to protect privacy that binds a government.

The convention facilitates the investigation and prosecution of cybercrime while requiring countries to have conditions and safeguards that adequately protect human rights.[55] The United States, for its part, has been pursuing CLOUD Act agreements to facilitate efficient access to electronic evidence stored in other countries in a manner that protects privacy and civil liberties.[56] In the EU, the E-Evidence Regulation enables law enforcement authorities in one of the bloc's member states to directly obtain electronic evidence from a provider in another. The regulation is premised "on the principle of mutual trust between the Member States and on a presumption of compliance by Member States with Union law, the rule of law and, in particular, with fundamental rights."[57] More work in this area is needed, but experience with the aforementioned approaches shows that concrete progress on cross-border data flows with trust is achievable and should inform future work on developing an overarching framework that is rights-protective, practicable, and scalable.

- **Building on the OECD TGA Declaration**. By identifying commonalities among like-minded democracies, the declaration establishes a baseline of safeguards and accountability mechanisms that OECD member countries have implemented as rights-protective and practicable.[58] With this baseline, participating governments identify concrete steps to help appropriate bodies "take into account a recipient country's effective implementation of the [OECD declaration's] principles."[59] Doing so can entail using the OECD declaration as a template for governments, in consultation with the private sector and civil society, to document how their legal frameworks align with

[55] Convention of Cybercrime, Nov. 23, 2011, ETS No. 185. https://rm.coe.int/1680081561

[56] US Department of Justice, Cloud Act Resources, March 8, 2023. https://www.justice.gov/criminal-oia/cloud-act-resources; The United States has entered into CLOUD Act Agreements with the United Kingdom and is in negotiations with Canada and the EU.

[57] REGULATION (EU) 2023/1543 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Recital 12. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1543&qid=1694434156917; See also Council of the EU, Council adopts EU laws on better access to electronic evidence, June 27, 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/

[58] In this manner, the declaration is akin to the OECD privacy guidelines set forth in 1980. Those guidelines, in turn, informed key privacy developments worldwide, including the APEC Privacy Framework (and Global CBPR), the EU's Data Protection Directive, and GDPR.

[59] OECD, supra note 24. "WE RECOGNISE that where our legal frameworks require that transborder data flows are subject to safeguards, our countries take into account a destination country's effective implementation of the [OECD declaration's] principles as a positive contribution towards facilitating transborder data flows in the application of those rules."

OECD principles.[60] Stakeholders should also identify practical examples of how governments demonstrate consistency with OECD principles.[61] Although the declaration was approved by the OECD's 38 member countries, it is important to note that the declaration refers to—and in vital ways is aligned with—the Global Privacy Assembly's 2021 resolution on government access to data, which identifies high-level principles that correspond with those in the OECD declaration. The Global Privacy Assembly comprises data protection and privacy authorities from around the world.

- **Enhancing international cooperation on oversight and redress.** A key element of establishing trust in cross-border data flows is enhancing understanding and cooperation among institutions involved in the oversight of and redress for government access issues. These institutions must also respect legitimate government needs to protect the secrecy of national security activities and the integrity of law enforcement investigations. Importantly, this does not require governments to share classified information outside normal channels. Rather, it involves establishing formalized communication and collaboration mechanisms so that oversight entities can better understand how rules are implemented, share good practices, and raise questions in an informed manner. Each country's oversight institutions should also be able to establish mechanisms to refer individual complaints and seek assistance with resolving those that involve data that crosses borders. Such cooperation should include establishing channels among national security and law enforcement oversight and redress institutions, on one hand, and government authorities responsible for making decisions on cross-border data flows (e.g., data protection authorities), on the other.[62]

---

[60] Government action is important here to ensure that relevant aspects of the legal framework are sufficiently transparent and readily understandable by external stakeholders, and engagement with experts in civil society is important to help determine the degree to which government characterizations are adequately substantiated with publicly available information. The governmental process should include engagement not only with officials responsible for national security and law enforcement activities and oversight, but also with agencies responsible for assessing recipient countries' privacy protections (e.g., data protection authorities) so that relevant government actors understand the extent to which the originating and recipient countries' laws align with OECD principles.

[61] For example, the United States created a new redress process for surveillance after questions were raised about the previous redress process. See Executive Order 14086, Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities, Section 3, Oct. 7, 2023. https://privacyacrossborders.org/wp-content/uploads/2022/10/Executive-Order-14086-on-Enhancing-Safeguards-for-United-States-Signals-Intelligence-Activities.pdf

[62] Such efforts should build on existing international initiatives. For data protection, for example, the Roundtable of G7 Data Protection and Privacy Authorities highlighted the work of the Global Privacy Assembly's International Enforcement Cooperation Working Group, the Global Privacy Enforcement Network, and the G7 Enforcement Cooperation Working Group. Supra note 2, ¶20-21. For national security, the International Intelligence Oversight Forum periodically gathers intelligence oversight representatives and national security officials from around the

Moving Forward with a Transparent and Inclusive Process

Stakeholders should establish an inclusive, multilateral process focused on commercial privacy and trusted government access. That process should seek agreement on a common benchmark for identifying democracies that respect the rule of law, a core set of rights-protective principles and accountability mechanisms, and practicable and scalable approaches.

What form should this process take? Although many options exist, it is important to start quickly, work multilaterally across sectors, and build on existing progress. The logical starting point, as noted, is the G7's commitment to operationalizing DFFT through a new dedicated IAP through which stakeholders can merge workflows into a more unified and harmonized effort. The new IAP should engender trust in participants' expertise, integrity, and commitment. The process, therefore, should be transparent to the public and include representatives from democracies worldwide (including countries that are not typically the focus of cross-border data flow discussions) and civil society.

The G7's recommendation to have the OECD lead on the IAP and pave the way toward operationalizing DFFT is logical for quickly starting the process.[63] The OECD is responsible for two key instruments that are directly relevant to DFFT, the OECD Privacy Guidelines and the TGA Declaration. It also has relevant institutional experience with these issues, an expert secretariat, and established methods for consulting with external stakeholders. To ensure transparency and inclusivity, however, the OECD must leverage its experience and processes to include non-member country participation, engage proactively with civil society and business organizations, and ensure open and frequent communication among other relevant international efforts.

The OECD, as an excellent starting point, need not, however, be the ending point. The G7 should continue to exercise leadership and evaluate whether future revisions to the IAP are needed to promote a rights-protective, practicable, and scalable framework open to all democracies that respect the rule of law.

---

world. See Council of Europe, Intelligence oversight in the Brave New World of Proportionality – 5th International Intelligence Oversight Forum (IIOF), Nov. 15, 2022. https://www.coe.int/en/web/data-protection/-/intelligence-oversight-in-the-brave-new-world-of-proportionality-5th-international-intelligence-oversight-forum-iiof-

[63] The G7 has turned to the OECD for other multilateral initiatives. The Global Partnership on AI, for example, "is an international and multistakeholder initiative to guide the responsible development and use of artificial intelligence consistent with human rights, fundamental freedoms and shared democratic values." OECD AI Policy Observatory, The Global Partnership on AI, https://oecd.ai/en/gpai; Ibid., It is "the fruition of an idea developed within the G7", and its secretariat is "hosted at the OECD." The initiative now includes 25 members.

Long-term Possibilities

Longer-term approaches could include establishing a new DFFT organization and secretariat, creating more international instruments, and expanding to other types of data or access. The authors believe that pushing forward now with the concrete steps outlined in this paper are important in their own right and are critical for laying a stronger path toward future efforts.

Annex A - List of Global Taskforce Participants

Bojana Bellamy, President, Centre for Information Policy Leadership
Mathias Cellarius, Group Data Protection Officer & Head of SAP Data Protection & Export Control, SAP SE
Anupam Chander, Professor of Law, Georgetown University
Theodore Christakis, Professor, University Grenoble Alpes (France) and Cross-Border Data Forum
Malcolm Crompton, Founder and Partner , IIS Partners
Jim Dempsey, Senior Policy Advisor, Program on Geopolitics, Technology and Governance, Stanford Cyber Policy Center
Christopher Docksey, Visiting Fellow, European Centre on Privacy and Cybersecurity, University of Maastricht Faculty of Law
Danilo Doneda, Professor, Instituto Brasiliense de Direito Publico
Caitlin Fennessy, Vice President & Chief Knowledge Officer, International Association of Privacy Professionals
Glenn Gerstell, Senior Advisor, Center for Strategic & International Studies
Robyn Greene, Head of Privacy Policy, Surveillance and Data Flows, Meta
Adam Klein, Director and Director of Program on Technology, Security and Global Affairs, Senior Lecturer in Law, Robert Strauss Center for International Security and Law, University of Texas at Austin
Christopher Kuner, Professor of Law, VUB Brussels, Co-Chair, Brussels Privacy Hub
Hosuk Lee-Makiyama, Director, Centre for European International Political Economy
Caroline Louveaux, Chief Privacy Officer, Mastercard
Orla Lynskey, Associate Professor of Law, London School of Economics Law School
Ricard Martinez, Constitutional Law Lecturer, University of Valencia, Director of the Privacy and Digital Transformation Chair, Microsoft-University of Valencia
Estelle Massé, Global Data Protection Lead, Access Now
Nohyoung Park, Dean, Korea University Law School, Director, Cyber Law Center
Carole Piovesan, Managing Partner, INQ Law
Alexandra Reeve Givens, President and CEO, Center for Democracy and Technology
Peter Swire, Elizabeth & Tommy Holder Chair of Law and Ethics, Scheller College of Business; Professor, School of Cybersecurity and Privacy, Georgia Institute of Technology
Thorsten Wetzling, Head of Research, Digital Rights, Surveillance and Democracy, Stiftung Neue Verantwortung
Joseph Whitlock, Director, Policy, BSA | The Software Alliance

Co-Chairs and Partners

Julie Brill, Chief Privacy Officer and Corporate Vice President, Global Privacy and Regulatory Affairs, Microsoft
Karen Kornbluh, Senior Fellow and Director, Digital Innovation and Democracy Initiative, The German Marshall Fund of the United States
Alex Joel, Senior Project Director and Adjunct Professor, Tech, Law & Security Program | Privacy Across Borders, American University Washington College of Law
Chris Calabrese, Senior Director, Global Privacy Policy, Microsoft