Atlantic Council
EUROPE CENTER

ISSUE BRIEF

Who's a National Security Risk? The Changing Transatlantic Geopolitics of Data Transfers

MAY 2024 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.

Introduction

The geopolitics of transatlantic data transfers have been unvarying for the past decade. European governments criticize the US National Security Agency (NSA) for exploiting personal data moving from Europe to the United States for commercial reasons. The US government responds, through a series of arrangements with the European Union, by providing assurances that NSA collection is not disproportionate, and that Europeans have legal avenues if they believe their data has been illegally used. Although the arrangements have not proven legally stable, on the whole they have sufficed to keep data flowing via subsea cables under the Atlantic Ocean.

Now the locus of national security concerns about international data transfers has shifted from Brussels to Washington. The Biden administration and the US Congress, in a series of bold measures, are moving aggressively to interrupt certain cross-border data flows, notably to China and Russia.

The geopolitics of international data flows remain largely unchanged in Europe, however. European data protection authorities have been mostly noncommittal about the prospect of Russian state surveillance collecting Europeans' personal data. Decisions on whether to transfer European data to Russia and China remain in the hands of individual companies.

Will Washington's new focus on data transfers to authoritarian states have an impact in Europe? Will Europe continue to pay more attention to the surveillance activities of its liberal democratic allies, especially the United States? Is there a prospect of Europe and the United States aligning on the national security risks of transfers to authoritarian countries?

Data transfer politics come to America

The US government long considered the movement of personal data across borders as primarily a matter of facilitating international trade.[1] US national security authorities' surveillance of foreigners' personal data in the course of commercial transfers was regarded as an entirely separate matter.

1 Kenneth Propp, "Transatlantic Digital Trade Protections: From TTIP to 'Policy Suicide?,'" *Lawfare*, February 16, 2024, https://www.lawfaremedia.org/article/transatlantic-digital-trade-protections-from-ttip-to-policy-suicide.

TikTok Chief Executive Officer Shou Zi Chew testifies before a House Energy and Commerce Committee hearing as lawmakers scrutinize the app. March 23, 2023. REUTERS/Evelyn Hockstein.

For example, the 2001 EU-US Safe Harbor Framework,[2] the first transatlantic data transfer agreement, simply allowed the United States to assert the primacy of national security over data protection requirements, without further discussion. Similarly, the 2020 US-Mexico-Canada Free Trade Agreement[3] and the US-Japan Digital Trade Agreement[4] contain both free flow of data guarantees and traditional national security carve-outs from those obligations.

Edward Snowden's 2013 revelations of expansive US NSA surveillance in Europe put the Safe Harbor Framework's national security derogation into the political spotlight. Privacy activist Max Schrems then challenged its legality under EU fundamental rights law, and the Court of Justice of the European Union (CJEU) ruled it unacceptable.[5]

The 2023 EU-US Data Privacy Framework[6] (DPF) is the latest response to this jurisprudence. In it, the United States commits to hold national security electronic surveillance of EU-origin personal data to a more constrained standard, as the European Commission has noted.[7] The United States' defensive goal has been to reassure Europe that it conducts foreign surveillance in a fashion that can be reconciled with EU fundamental rights law.

Now, however, the US government has begun expressly integrating its own national security considerations into decisions on the foreign destinations to which US-origin personal data may flow. It is a major philosophical shift from the prior free data flows philosophy, in which national security limits played a theoretical and marginal role.

One notable development is a February 28, 2024, executive order, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.[8] The EO empowers the Department of Justice (DOJ), in consultation with other relevant departments, to identify countries "of concern" and to prohibit or otherwise regulate bulk data transfers to them, based on a belief that these countries could be collecting such data for purposes of spying on or extorting Americans. A week later DOJ issued a proposed rule describing the envisaged regulatory regime, and proposing China, Cuba, Iran, North Korea, Russia, and Venezuela as the countries "of concern."[9]

The White House, in issuing the bulk data EO, was at pains to insist that it was limited in scope and not inconsistent with the historic US commitment to the free flow of data, because it applies only to certain categories of data and certain countries.[10] Nonetheless, as has been observed by scholars Peter Swire and Samm Sacks, the EO and proposed rule are, for the United States, part of "a new chapter in how it regulates data flows" in that they would create an elaborate new national security regulatory regime applying to legal commercial data activity.[11]

European Commission Vice President for Values and Transparency Věra Jourová and then-European Commissioner for Justice Didier Reynders speak about the EU's GDPR rules. June 24, 2020. REUTERS/Olivier Hoslet.

2 *U.S.-EU Safe Harbor Framework: Guide to Self-Certification*, US Department of Commerce, March 2009, https://legacy.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf.

3 "Chapter 19: Digital Trade," US-Mexico-Canada Free Trade Agreement, Office of the United States Trade Representative, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

4 "Agreement between the United States of America and Japan Concerning Digital Trade," Office of the United States Trade Representative, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

5 Schrems v. Data Protection Commissioner, CASE C-362/14 (Court of Justice of the EU 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362.

6 "President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework," Fact Sheet, White House Briefing Room, October 7, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

7 European Commission, "Commission Implementing Decision of 10.7.2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data under the EU-US Data Privacy Framework," July 10, 20203 https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

8 Exec. Order No. 14117, 89 Fed. Reg. 15421 (2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

9 Department of Justice, "National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern," Proposed Rule, 28 C.F.R. 202 (2024), https://www.federalregister.gov/d/2024-04594.

10 "President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data," Fact Sheet, White House Briefing Room, February 28, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

11 Peter Swire and Samm Sacks, "Limiting Data Broker Sales in the Name of U.S. National Security: Questions on Substance and Messaging," *Lawfare*, February 28, 2024, https://www.lawfaremedia.org/article/limiting-data-broker-sales-in-the-name-of-u.s.-national-security-questions-on-substance-and-messaging.

Hard on the heels of the bulk data EO came congressional passage in April of the Protecting Americans' Data from Foreign Adversaries Act, which the president signed into law.[12] It prohibits data brokers from selling or otherwise making available Americans' sensitive information to four specified countries: China, Iran, North Korea, and Russia. The new law has a significantly broader scope than the EO. It cuts off certain data transfers to any entity controlled by one of these adversary countries, apparently including corporate affiliates and subsidiaries. It extends to any sensitive data, not just data in bulk. It remains to be seen how the administration will address the overlaps between the new law and the EO.

Another part of the same omnibus legislation ordered the ban or forced sale of TikTok, the Chinese social media platform widely used in this country.[13] Advocates of the law point to the government of China's ability under its own national security law to demand that companies operating there turn over personal data, including, potentially, TikTok users' data transferred from the United States. Critics have cast the measure as a targeted punishment of a particular company, done without public evidence being offered of national security damage. TikTok has challenged the law as a violation of the First Amendment.[14]

Finally, the data transfer restrictions in these measures are thematically similar to a January 29 proposed rule from the Commerce Department obliging cloud service providers to verify the identity of their customers, on whose behalf they transfer data.[15] The rule would impose know your customer (KYC) requirements—similar to those that apply in the international banking context—for cloud sales to non-US customers, wherever located.

This extraordinary burst of legislative and executive action focused on the national security risks of certain types of data transfers from the United States to certain authoritarian states is indicative of how far and fast political attitudes have shifted in this country. But what of Europe, which faces similar national security data challenges from authoritarian states? Is it moving in a similar direction as the United States?

Data transfer politics in Europe

The EU, unlike the United States, has long had a systematic set of controls on personal data flows from EU territory abroad, articulated in the General Data Protection Regulation (GDPR).[16] The GDPR conditions transfers to a foreign jurisdiction on the "adequacy" of its data protection safeguards—or, as the CJEU has refined the concept, their "essential equivalence" to the GDPR regime.

The task of assessing foreign legal systems falls to the European Commission, the EU's quasi-executive arm. Article 45 of the GDPR instructs it to consider, among other things, "the rule of law, respect for human rights and fundamental freedoms, relevant legislation . . . including concerning . . . the access of public authorities to personal data."

For much of the past decade, the central drama in the European Commission's adequacy process has been whether the United States meets this standard. As previously noted, the CJEU invalidated first the Safe Harbor Framework,[17] in 2015, and then the Privacy Shield Framework,[18] in 2020. The DPF is the third try by the US government and the European Commission to address the CJEU's fundamental rights concerns. Last year, the European Commission issued yet another adequacy decision that found the DPF adequate.[19] The EU understandably has focused its energies on the United States, since vast amounts of Europeans' personal data travels to cloud service providers' data centers in the United States and, as Snowden revealed, offered an inviting target for the NSA.

Separately, the European Commission has gradually expanded the range of other countries benefiting from adequacy findings, conferring this status on Japan,[20] Korea,[21] and the United Kingdom.[22] However, the 2019 adequacy decision for the UK continues to be criticized in Brussels. On April 22, the Committee on Civil Liberties, Justice, and Home Affairs (LIBE) of the European Parliament wrote to the UK House of Lords complaining about UK national security bulk data collection practices and the prospect of onward transfer of data from UK territory to jurisdictions

12 "Protecting Americans from Foreign Adversary Controlled Applications Act," in emergency supplemental appropriations, Pub. L. No. 118–50, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/7520/text.

13 Cristiano Lima-Strong, "Biden Signs Bill That Could Ban TikTok, a Strike Years in the Making," *Washington Post*, April 24, 2024, https://www.washingtonpost.com/technology/2024/04/23/tiktok-ban-senate-vote-sale-biden/.

14 "Petition for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act," TikTok Inc. and ByteDance Ltd. v. Merrick B. Garland (US Court of Appeals for the District of Columbia Cir. 2024), https://sf16-va.tiktokcdn.com/obj/eden-va2/hkluhazhjeh7jr/AS%20FILED%20TikTok%20Inc.%20and%20ByteDance%20Ltd.%20Petition%20for%20Review%20of%20H.R.%20815%20(2024.05.07)%20(Petition).pdf?x-resource-account=public.

15 Department of Commerce, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," Proposed Rule, 15 C.F.R. Part 7 (2024), https://www.govinfo.gov/content/pkg/FR-2024-01-29/pdf/2024-01580.pdf.

16 "Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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)," 2016/679, Official Journal of the European Union (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

17 Schrems v. Data Protection Commissioner.

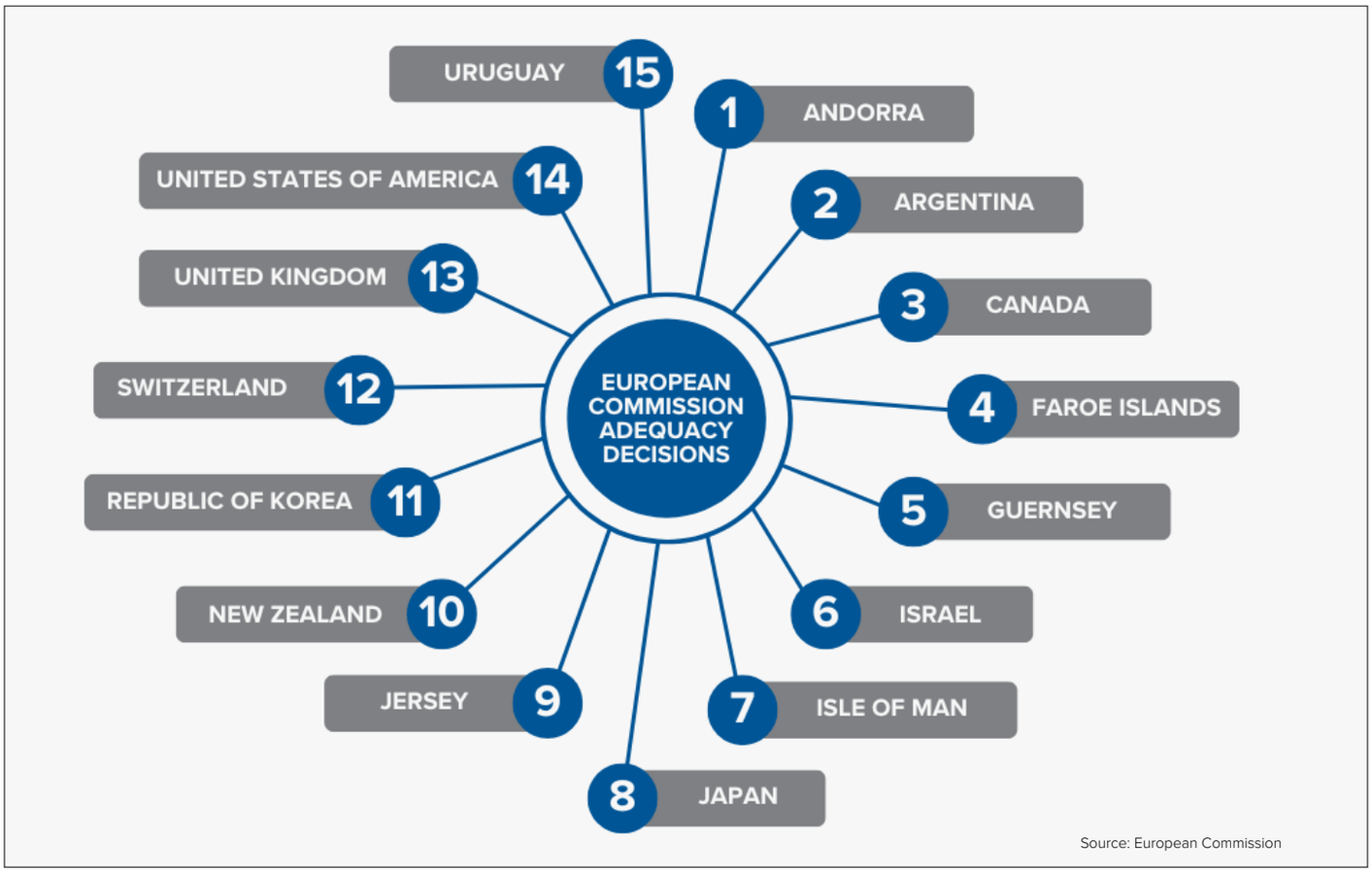
18 Data Protection Commissioner v. Facebook Ireland & Schrems, CASE C-311/18 (Court of Justice of the EU 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311.

19 The Commission's decision has since been challenged before the CJEU. See Latombe v. Commission, No. Case T-553/23 (Court of Justice of the EU 2023), https://curia.europa.eu/juris/document/document.jsf?text=&docid=279601&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1498741.

20 European Commission, "European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows," Press Release, January 23, 2019, https://commission.europa.eu/document/download/c2689793-a827-4735-bc8d-15b9fd88e444_en?filename=adequacy-japan-factsheet_en_2019.pdf.

21 "Commission Implementing Decision (EU) 2022/254 of 17 December 2021 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the Republic of Korea under the Personal Information Protection Act," Official Journal of the European Union, December 17, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D0254.

22 "Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom," Official Journal of the European Union, June 28, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D1772.



Source: European Commission

not deemed adequate by the EU.[23] Next year, the European Commission will formally review the UK's adequacy status.

This past January, the European Commission renewed the adequacy decisions for eleven jurisdictions which had long enjoyed them, including, notably, Israel.[24] On April 22, a coalition of civil society groups published an open letter to the European Commission questioning the renewal of Israel's adequacy decision.[25] The letter expressed doubts about the rule of law in Israel itself, the specific activities of Israeli intelligence agencies in Gaza during the current hostilities there, and the surveillance powers exercised by those agencies more generally.

Also delicate is the continuing flow of personal data from the European Union to Russia and China. Although neither country has been—or is likely to be—accorded adequacy status, data nonetheless can continue to flow to their territories, as to other third countries, if accompanied by contractual data protection safeguards. The CJEU established in its *Schrems* jurisprudence that such standard contractual clauses (SCCs) must uphold the same fundamental rights standards as an adequacy decision. The European Data Protection Board (EDPB) subsequently issued detailed guidance on the essential guarantees against national security surveillance that must be in place in order for personal data to be sent to a nonadequate jurisdiction.[26]

In 2021, the EDPB received an outside expert report[27] on several foreign governments' data access regimes. Its findings were clear. "Chinese law legitimises broad and unrestricted access to personal data by the government," it concluded. Similarly, with respect to Russia, "The right to privacy is strongly limited when interests of national security are at stake." The board did not take any further steps to follow up on the report, however.

23 European Parliament Justice Committee, Correspondence to Rt. Hon. Lord Peter Ricketts regarding Inquiry into Data Adequacy, April 22, 2024, https://content.mlex.com/Attachments/2024-04-25_L75P-CWU60ZLVILJ5%2FLIBE%20letter%20-%20published%20EAC.pdf.

24 "Report from the Commission to the European Parliament and the Council on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) of Directive 95/46/EC," European Commission, January 15, 2024, https://commission.europa.eu/document/download/f62d70a4-39e3-4372-9d49-e59dc0fda3df_en?filename=JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf.

25 European Digital Rights et al., Letter to Vice-President of the European Commission Věra Jourová Regarding Concerns following Reconfirmation of Israel's Adequacy Status, April 22, 2024, https://edri.org/wp-content/uploads/2024/04/Concerns-Regarding-European-Commissions-Reconfirmation-of-Israels-Adequacy-Status-in-the-Recent-Review-of-Adequacy-Decisions-updated-open-letter-April-2024.pdf.

26 Milieu Consulting and Centre for IT and IP Law of KU Leuven, "Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures," Prepared for European Data Protection Board (EDPB), November 10, 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

27 Milieu Consulting and Centre for IT and IP Law of KU Leuven, "Government Access to Data in Third Countries," EDPB, EDPS/2019/02-13, November 2021, https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.

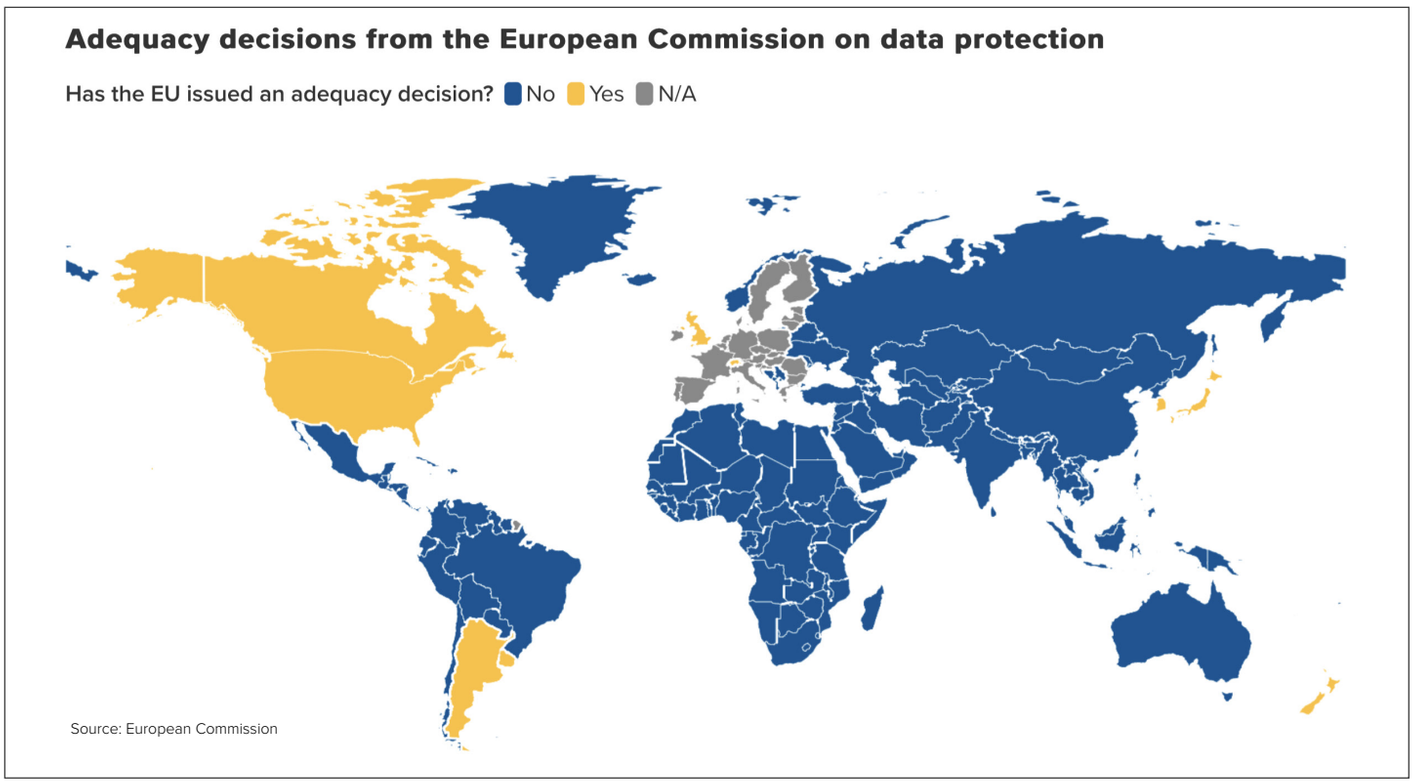
Shortly after Russia invaded Ukraine, Russia was excluded from the Council of Europe and ceased to be a party to that body's European Convention on Human Rights.[28] The European Data Protection Board issued a statement confirming that data transfers to Russia pursuant to standard contract clauses remained possible, but stressed that safeguards to guard against Russian law enforcement or national security access to data were vital.[29]

Over two thousand multinational companies continue to do business in Russia, despite the Ukraine war, although a smaller number have shut down, according to a Kyiv academic research institute.[30] Data flows between Europe and Russia thus remain substantial, if less than previously. Companies engaged in commerce in Russia also are subject to requirements that data on Russian persons be localized in that country.[31] Nonetheless, data flows from Europe to Russia are not subject to categorical exclusions, unlike the new US approach.

The sole reported case of a European data protection authority questioning data flows to Russia involves Yango, a taxi-booking mobile app developed by Yandex, a Russian internet search and information technology company. Yango's European services are based in the Netherlands and are available in other countries including Finland and Norway. In August 2023, Finland's data protection authority (DPA) issued an interim decision to suspend use of Yango in its territory because Russia had just adopted a decree giving its state security service (FSB) unrestricted access to commercial taxi databases.[32]

The interim suspension decision was short-lived. A month later, the Finnish authority, acting in concert with Norwegian and Dutch counterparts, lifted it, on the basis of a clarification that the Russian decree in fact did not apply to use of the Yango app in Finland.[33] The Finnish authority further announced that the Dutch authority, in coordination with it and Norway, would issue a final decision in the matter. The Dutch investigation reportedly remains open, but it does not appear to be a high priority matter.

The day after lifting the Yango suspension, the Finnish data protection authority rushed out yet another press release advising



28 European Convention on Human Rights, November 4, 1950, https://www.echr.coe.int/documents/d/echr/Convention_ENG.

29 Statement 02/2022 on Data Transfers to the Russian Federation, European Data Protection Board, July 12, 2022, https://www.edpb.europa.eu/system/files/2022-07/edpb_statement_20220712_transfersto-russia_en.pdf.

30 "Stop Doing Business with Russia," KSE Institute, May 20, 2024, #LeaveRussia: The List of Companies that Stopped or Still Working in Russia (leave-russia.org).

31 "Russian Data Localization Law: Now with Monetary Penalties," Norton Rose Fulbright Data Protection Report, December 20, 2019, https://www.dataprotectionreport.com/2019/12/russian-data-localization-law-now-with-monetary-penalties/.

32 "Finnish DPA Bans Yango Taxi Service Transfers of Personal Data from Finland to Russia Temporarily," Office of the Data Protection Ombudsman, August 8, 2023, https://tietosuoja.fi/en/-/finnish-dpa-bans-yango-taxi-service-transfers-of-personal-data-from-finland-to-russia-temporarily.

33 "European Data Protection Authorities Continue to Cooperate on the Supervision of Yango Taxi Service's Data Transfers–Yango Is Allowed to Continue Operating in Finland until Further Notice," Office of the Data Protection Ombudsman, September 26, 2023, https://tietosuoja.fi/en/-/european-data-protection-authorities-continue-to-cooperate-on-the-supervision-of-yango-taxi-service-s-data-transfers-yango-is-allowed-to-continue-operating-in-finland-until-further-notice.

that its decision "does not address the legality of data transfers to Russia," or "mean that Yango data transfers to Russia would be in compliance with the GDPR or that Russia has an adequate level of data protection."[34]

One can interpret this final Finnish statement as at least indirectly acknowledging that continued commercial data transfers from an EU jurisdiction to Russia may raise rule of law questions bigger than a single decree allowing its primary security agency, known as the FSB, to access certain taxi databases. Otherwise, the Finnish decision could be criticized for ignoring the forest for the birch trees.

Equally striking is the limited extent of DPA attention to data transfers between EU countries and China. China maintains an extensive national security surveillance regime, and lately has implemented a series of legal measures that can limit outbound data transfers for national security reasons.[35] In 2023, the Irish Data Protection Commissioner[36] imposed a substantial fine on TikTok for violating the GDPR with respect to children's privacy, following a decision by the EDPB.[37] This inquiry did not examine the question of whether Chinese government surveillance authorities had access to European users' data, however.

Personal data actively flows between Europe and China in the commercial context, pursuant to SCCs. China reportedly may issue additional guidance to companies on how to respond to requests for data from foreign law enforcement authorities. To date there is no public evidence of European DPAs questioning companies about their safeguard measures for transfers to China.

Indeed, signs recently have emerged from China of greater openness to transfers abroad of data generated in the automotive sector, including from connected cars. Data from connected cars is a mix of nonpersonal and personal data. China recently approved Tesla's data security safeguards, enabling

34 "The Data Protection Ombudsman's Decision Does Not Address the Legality of Data Transfers to Russia–the Matter Remains under Investigation," Office of the Data Protection Ombudsman, September 27, 2023, https://tietosuoja.fi/en/-/the-data-protection-ombudsman-s-decision-does-not-address-the-legality-of-data-transfers-to-russia-the-matter-remains-under-investigation#:~:text=The%20Office%20of%20the%20Data%20Protection%20Ombudsman%27s%20decision,Protection%20Ombudsman%20in%20October%2C%20was%20an%20interim%20decision.

35 Samm Sacks, Yan Lou, and Graham Webster, "Mapping U.S.-China Data De-Risking," Freeman Spogli Institute for International Studies, Stanford University, February 29, 2024), https://digichina.stanford.edu/wp-content/uploads/2024/03/20240228-dataderisklayout.pdf.

36 "Irish Data Protection Commission Announces €345 Million Fine of TikTok," Office of the Irish Data Protection Commissioner, September 15, 2023, https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.

37 "Following EDPB Decision, TikTok Ordered to Eliminate Unfair Design Practices Concerning Children," European Data Protection Board, September 15, 2023, https://www.edpb.europa.eu/news/news/2023/following-edpb-decision-tiktok-ordered-eliminate-unfair-design-practices-concerning_en.

US and EU officials speak at a meeting of the US-EU Trade and Technology Council in Washington, DC. January 30, 2024. REUTERS/Leah Millis.

the company's previously localized data to leave the country.[38] In addition, the government of Germany is trying to ease the passage of data to and from China on behalf of German carmakers. On April 16, several German government ministers, part of a delegation visiting China led by Chancellor Olaf Scholz, issued a joint political statement with Chinese counterparts promising "concrete progress on the topic of reciprocal data transfer—and this in respect of national and EU data law," with data from connected cars and automated driving in mind.[39]

Conclusions

The United States and the European Union are, in some respects, converging in their international data transfer laws and policies. In Washington, free data transfers are no longer sacrosanct. In Europe, they never have been. Viewed from Brussels, it appears that the United States is, finally, joining the EU by creating a formal international data transfers regime—albeit constructed in a piecemeal manner and focused on particular countries, rather than through a comprehensive and general data privacy law.

Yet the rationales for limiting data transfers vary considerably from one side of the Atlantic to the other. Washington now focuses on the national security dangers to US citizens and to the US government from certain categories of personal data moving to the territories of "foreign adversaries." Brussels instead applies more abstract criteria relating to foreign governments' commitment to the rule of law, human rights, and especially their access to personal data.

A second important difference is that the United States has effectively created a blacklist of countries to which certain categories of data should not flow, whereas the EU's adequacy process serves as a means of "white listing" countries with comparable data protection frameworks to its own. Concretely, this structural difference means that the United States concentrates on prohibiting certain data transfers to China and Russia, while the EU institutionally has withheld judgment about transfers to those authoritarian jurisdictions. Critics of the EU's adequacy practice instead have tended to concentrate on the perceived risks of data transfers to liberal democracies with active foreign surveillance establishments: Israel, the United Kingdom, and the United States.

The transatlantic—as well as global—geopolitics of data transfers are in flux. The sudden US shift to viewing certain transfers through a national security lens is unlikely to be strictly mirrored in Europe. In light of the emerging differences in approach, the United States and European governments should consider incorporating the topic of international data transfers into existing political-level conversations. Although data transfer topics have thus far not figured into the formal work of the EU-US Trade and Technology Council (TTC),[40] which has met six times since 2022 including most recently in April,[41] there is no evident reason why that could not change. If the TTC resumes activity after the US elections, it could become a useful bilateral forum for candid discussion of perceived national security risks in data flows.

Utilizing a broader grouping, such as the data protection and privacy authorities of the Group of Seven (G7), which as a group has been increasingly active in the last few years,[42] also could be considered. The deliberations of this G7 group already have touched generally on the matter of government access, and they could readily expand to how its democratic members assess risks from authoritarians in particular. Eventually, such discussions could be expanded beyond the G7 frame into broader multilateral fora. The Organisation of Economic Co-operation and Development (OECD) Declaration on Government Access[43] is a good building block.

The days when international data transfers were a topic safely left to privacy lawyers are long gone. It's time for Washington and Brussels to acknowledge that the geopolitics of data flows has moved from the esoteric to the mainstream, and to grapple with the consequences.

38 "Tesla Reaches Deals in China on Self-Driving Cars," New York Times, April 29, 2024, https://www.nytimes.com/2024/04/29/business/elon-musk-tesla-china-full-self-driving.html.

39 "Memorandum of Understanding with China," German Federal Ministry of Digital and Transport, April 16, 2024, https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2024/021-wissing-deutschland-china-absichtserklaerung-automatisiertes-und-vernetztes-fahren.html.

40 Frances Burwell and Andrea Rodríguez, "The US-EU Trade and Technology Council: Assessing the Record on Data and Technology Issues," Atlantic Council, April 20, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/us-eu-ttc-record-on-data-technology-issues/.

41 "U.S.-EU Trade and Technology Council (TTC)," US State Department, https://www.state.gov/u-s-eu-trade-and-technology-council-ttc/.

42 "G7 DPAs' Action Plan," German Office of the Federal Commissioner for Data Protection and Freedom of Information (BfDI), June 22, 2023, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/2023-Action-Plan.pdf?__blob=publicationFile&v=1.

43 OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, December 14, 2022, OECD/LEGAL/0487, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

About the author

Kenneth Propp is a nonresident senior fellow with the Atlantic Council's Europe Center. He is also 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 to 2015, he served as legal counselor at the US Mission to the European Union (EU) in Brussels where he led US government engagement on privacy law and policy and digital regulation, and advised on trade negotiations with the EU.

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
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Alain Bejjani
Colleen Bell
Sarah E. Beshar
Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*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
Stuart E. Eizenstat
Tara Engel
Mark T. Esper
Christopher W.K. Fetzer
*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
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
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
Roger R. Martella Jr.
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
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
Elizabeth Frost Pierson
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Francesco G. Valente
Melanne Verveer
Tyson Voelkel
Kemba Walden
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Alan Yang
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 24, 2024

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