Atlantic Council

SOUTH ASIA CENTER

ISSUE BRIEF

Trading in US-India Data Flows

Prospects for Cooperation in US-India Data Policy

MARCH 2022

JUSTIN SHERMAN

Executive Summary

With a new US administration, movement on India's Personal Data Protection Bill, and a reinvigorated US-India Trade Policy Forum, the United States and India have a renewed opportunity to engage in dialogues and pursue cooperation on cross-border data flow and data privacy policy. Yet, many ideological and structural differences between the United States and India—including a lack of strong US privacy laws, India's push for data localization, and Indian views of data sovereignty and digital colonialism—present many challenges to cooperation. This issue brief, therefore, overviews the state of US, Indian, and US-India cross-border data flow and data policy, and discusses opportunities for cooperation and sources of contestation. It ultimately recommends the United States and India convene bilateral dialogues focused on tangible, near-term objectives in three areas: law enforcement access to data; definitions of, and exceptions to, data processing and localization requirements; and cybersecurity of data.

Introduction

As the Joe Biden administration and the Narendra Modi government reconvene the US-India Trade Policy Forum (TPF) after a four-year hiatus, one digital issue set remains central to challenges and opportunities in US-India trade: cross-border data flows and data policy. These issues received some attention under the Donald Trump administration, but the combination of a new US administration, key developments in Indian

The Atlantic Council's **South Asia Center** serves as the Atlantic Council's focal point for work on the region as well as relations between these countries, neighboring regions, Europe, and the United States. With the intersection of South Asia and its geopolitics at the center of SAC's vision, we work to find multilateral solutions to South Asia's most vital challenges.

The **US-India trade initiative**, housed within the South Asia Center, seeks to generate and disseminate innovative policy ideas that will inform future as well as ongoing trade negotiations between the United States and India and efforts to build a new digital trade agenda for a free and open Indo-Pacific.

cross-border data flow and data policies, and rising global calls for data privacy and data localization rules make this a unique and important moment for the two powers. With leading technology sectors, strong political influence, and some of the largest economies on the planet, the United States and India have real opportunities to identify common ground on data policy and work to maximize the mutual benefits therein. Yet, key political and ideological differences—particularly around data localization and ideas of data sovereignty—will challenge the United States and India to focus on areas of cooperation with potential for tangible, near-term achievements, rather than attempting to address every data issue at once.

Following the November 2021 TPF meeting in New Delhi, the United States and India released a joint statement affirming (among other things) that they would "deepen bilateral engagement to promote the digital economy, and to explore the adoption of joint principles that ensure that the internet remains open for free exchange of ideas, goods, and services."[1] The TPF ministers also highlighted "the important role of the services sector, including digital services, in India and the United States, and the significant potential for increasing bilateral services trade and investment." It followed President Biden and Prime Minister Modi declaring at a September 2021 meeting that they would "develop an ambitious, shared vision for the future of the trade relationship."[2]

The United States and India face many challenges within the cross-border data flow and data policy issue set. US tech companies, as well as the Trump and Biden administrations, have lobbied against proposed data localization requirements in India, in which data on Indian citizens would be subject to various local storage rules and restrictions on transfer outside India. The Modi government, for its part, is working on bolstering domestic technology growth, and members of parliament drafting India's Personal Data Protection Bill appear committed to imposing data localization requirements and designing a "new" data model for Global South countries (in contrast to those for the European Union, China, and the United States). Ahead of the TPF's reconvening in March 2022, there is much for the United States and India to weigh on data policy. The shape of US-India data policy in the next few years will have significant impacts on citizen and consumer privacy, economic growth and competitiveness, and national security as rules on data collection, storage, processing, and transfer impact everything from consumer financial transactions to healthcare and medicinal research to law enforcement data access.

This issue brief details opportunities for cooperation and sources of contestation in US-India data policy. It then recommends that the United States and Indian governments convene bilateral dialogues focused narrowly on achieving tangible, near-term objectives on data policy. These bilateral dialogues should focus initially on three key areas, including:

- law enforcement access to data;
- definitions of and exceptions to data processing and localization requirements; and
- cybersecurity of data.

US-India Cooperation and Contestation

India is developing a Personal Data Protection Bill to create an Indian data privacy framework, and the United States still does not have a comprehensive federal consumer privacy law. Simultaneously, new data privacy frameworks in other parts of the world (e.g., Brazil) impact cross-border data flows for the United States and India.[3] The same goes for the sixty-two countries that now have data localization restrictions, as well as the parts of the world considering them (e.g., the European Union).[4] While the United States and India are engaged in several bilateral and multilateral dialogues around data policy issues, key challenges remain around Indian law enforcement access to data, the lack of a strong US privacy law, and Indian data localization proposals.

In December 2019, a draft Personal Data Protection Bill was introduced into Indian parliament, which set out to create a

1 "Joint Statement from the United States—India Trade Policy Forum," Office of the United States Trade Representative, November 23, 2021, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/november/joint-statement-united-states-india-trade-policy-forum.

2 Ibid.

3 "Brazilian General Data Protection Law (LGPD, English translation)," International Association of Privacy Professionals, October 2020, https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

4 Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology & Innovation Foundation, July 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost; Peter Swire and DeBrae Kennedy-Mayo, "Hard Data Localization May Be Coming to the EU—Here are 5 Concerns," International Association of Privacy Professionals, January 26, 2021, https://iapp.org/news/a/hard-data-localization-may-be-coming-to-the-eu-here-are-five-concerns/.

comprehensive data privacy framework for Indian citizens and establish a Data Protection Authority to carry out enforcement.[5] The bill was referred to a Joint Parliamentary Committee for review, which released its much awaited and somewhat delayed report on the bill in December 2021.[6] While some of the bill's provisions echo those in the EU's General Data Protection Regulation (GDPR), such as altered versions of consent and notification provisions, others are distinct. Notably, it includes data localization requirements—which would require data on Indian citizens held by the Indian government, domestic companies, and foreign companies to be stored in India. The initially proposed localization rules were relaxed in a revised draft, but they would still require that some kinds of data have copies stored in India ("mirroring"), while other kinds of data be stored locally with restrictions on outbound transfer ("hard localization"). The bill also, troublingly, contains broad and vague carveouts for the government to access, use, and store data on Indian citizens.[7] In similar form, the revised draft would concerningly allow the government to compel companies to hand over "non-personal data" for the broadly defined objectives of delivering more targeted services or formulating "evidence-based policies by the Central government."[8]

The United States still does not have a comprehensive federal consumer privacy law. US companies can legally buy and sell individuals' intimate personal data on the open market, and—outside of stricter sectoral rules such as in healthcare—there are few meaningful restrictions on companies collecting data on consumers.[9] However, there have been key developments in US data policy with other countries. In 2018, the United States enacted the CLOUD Act, which asserted the US government's right to compel access to data stored overseas by US companies and authorized the executive branch to make agreements with foreign governments on law enforcement data access requests, bypassing Mutual Legal Assistance Treaty (MLAT) processes.[10] The United States currently does not have a CLOUD Act agreement with India, which could help address Indian frustrations with the slow, inefficient MLAT process for law enforcement to access US company-held data (discussed more below).[11] Despite US efforts to renegotiate Privacy Shield and to forge data policy cooperation with foreign partners, such as through the EU-US Trade and Technology Council, the results of those efforts remain to be seen, though there is some indication the United States and European Union (EU) may be nearing a new data transfer agreement.

Data localization is one of the biggest points of data policy contestation between the United States and India. At the 2019 Group of Twenty (G20) meeting in Osaka, Japan, then President Trump said that "the United States opposes data localization and policies, which have been used to restrict digital trade flows and violate privacy and intellectual property protections."[12] Before that, the US ambassador to India said countries should "avoid overreaching on policies such as data localization."[13] This has continued in the new administration, as the executive branch and Congress have remained critical of data localization requirements in India and elsewhere.[14] Large US technology companies have also been resolute in their opposition to the localization requirements, which could alter the current flow of data across

5 "Personal Data Protection Bill," 2019, https://drive.google.com/file/d/1vmeCRehq7eiURstOhnio_UTaCkSgM5gv/view. See a concise summary at: "The Personal Data Protection Bill, 2019," PRS Legislative Research, last visited January 3, 2021, https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.

6 "Report of the Joint Committee on the Personal Data Protection Bill, 2019," Lok Sabha, December 2021. https://www.ahlawatassociates.com/wp-content/uploads/2021/12/17-Joint-Committee-on-the-Personal-Data-Protection-Bill-2019.pdf.

7 "Personal Data Protection Bill."

8 See, e.g., an explainer: Apoorva Mandhani, "Non-personal Data, Social Media—What New 'Data Protection Bill' Could Look Like," *Print*, December 6, 2021, https://theprint.in/theprint-essential/non-personal-data-social-media-what-new-data-protection-bill-could-look-like/776389/.

9 Justin Sherman. Written testimony to the Senate Committee on Finance. Subcommittee on Fiscal Responsibility and Economic Growth. Hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector," December 7, 2021, https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf.

10 "Division V—Cloud Act," US Department of Justice, last visited March 7, 2022, https://www.justice.gov/dag/page/file/1152896/download; Jennifer Daskal, "Unpacking the CLOUD Act," *European Criminal Law Association,* 4, 2018, 220–225.

11 For interesting discussion of India and the CLOUD Act in general, see: Elonnai Hickok and Vipul Kharbanda, "An Analysis of the CLOUD Act and Implications for India," Centre for Internet & Society, August 2018, https://cis-india.org/internet-governance/blog/an-analysis-of-the-cloud-act-and-implications-for-india.

12 Justin Sherman, "The US Is Waging War on Digital Trade Barriers," *WIRED*, April 10, 2020, https://www.wired.com/story/the-us-is-waging-war-on-digital-trade-barriers/; "Remarks by Ambassador Juster at Indo-American Chamber of Commerce Annual Convention Inaugural Session," US Embassy & Consulates in India, September 21, 2018, https://in.usembassy.gov/remarks-by-ambassador-kenneth-i-juster-at-the-indo-american-chamber-of-commerce-iacc-annual-convention-inaugural-session/.

13 Ibid.

14 "2021 National Trade Estimate Report on Foreign Trade Barriers," Office of the United States Trade Representative, March 2021, 102, 104, 157, 215, 266, 267, https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf.

borders and raise the cost of doing business in India for both domestic and foreign companies (in the way of technical and legal compliance costs).[15] For instance, Mastercard, Visa, and American Express attempted to weaken or entirely reverse, to no avail, the Reserve Bank of India's 2018 decision to make foreign payment firms store payment data on Indians domestically.[16]

On the flip side, Indian policymakers have expressed a multitude of views on data localization. Some policymakers have embraced a view of "data sovereignty" where the Indian state must assert technical and legal control over data flows through localization requirements. This mainly concerns political sovereignty in the digital sphere. Related, but distinct, the data localization rules in India's Personal Data Protection Bill are also driven by the concept of "digital colonialism," where large and globally dominant US technology firms enter the Indian market, collect data on Indian citizens, and extract all the economic value back to the United States.[17] Mukesh Ambani, chairman and managing director of Reliance Industries and one of the richest people in India, has himself said that "data colonization" is as bad as other forms of colonization and that "India's data must be controlled and owned by Indian people and not by corporates, especially global corporations."[18] Data localization is also, therefore, a pushback against this US technology power via cost imposition—and, as outlined in India's 2019 Draft e-Commerce Policy, a way to supposedly boost the growth of domestic technology players in tandem.[19] The Joint Parliamentary Committee report on the bill writes that localization will "substantially" enhance data center infrastructure in India by encouraging both domestic and foreign firms to make greater investments.[20] Alongside this, the Indian Ministry of Electronics and Information Technology drafted a Data Center Policy in 2020 aimed at boosting domestic data center infrastructure, including because of proposed data localization requirements and "protection of the digital sovereignty of the country."[21]

Law enforcement access to data is also a key driver of data localization proposals—and is itself a key issue in US-India data policy. In most cases, Indian law enforcement must request data from US companies for criminal investigations by filing MLAT requests with the Justice Department. However, this process has been slow and inefficient; in fact, Indian law enforcement has recently begun filing some of these requests directly to US companies, especially a few of the large social media and internet platforms, even if companies often do not hand over the data. This inefficiency has also led some Indian policymakers to view data localization as a way to try to ensure law enforcement access to data on Indian citizens. The Joint Parliamentary Committee report states outright, "Data localization would lead to easier access to data for the Government and law enforcement agencies, thus facilitating better law enforcement."[22]

Lastly, data localization is driven by domestic and international political positioning. Some Indian legislators, as mentioned, want to impose costs on US technology firms as part of pushing back against digital colonialism. The Modi government, specifically, is also driven by its desire to assert control over foreign (largely, US) data-driven businesses, including social media platforms, which it has repeatedly forced or tried to force to censor information

15 On costs, see: DeBrae Kennedy-Mayo, Peter Swire, and Michael Young, "IRSG Issues Report Critical of Data Localization Impacts on Financial Sector," Cross-Border Data Forum, March 11, 2021, https://www.crossborderdataforum.org/irsg-issues-report-critical-of-data-localization-impacts-on-financial-sector/; Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology & Innovation Foundation, May 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

16 Aditya Kalra and Manoj Kumar, "India to Review Data Storage Rules that Irked U.S. Tech Firms," Reuters, June 18, 2019, https://www.reuters.com/article/us-india-data-localisation/india-to-review-data-storage-rules-that-irked-u-s-tech-firms-idUSKCN1TJ0WN.

17 This idea is not confined to India, as more research, advocacy, and thinking are produced on notions of data colonialism, digital colonialism, and decolonization in the digital age. See, e.g.: Nick Couldry and Ulises Ali Mejias, "The Decolonial Turn in Data and Technology Research: What Is at Stake and Where Is It Heading?" *Information, Communication & Society,* 2021; Shruti Dhapola, "Digital Colonisation: How Indian Languages Lost out to English on the Internet," *Indian Express*, November 20, 2020, https://indianexpress.com/article/technology/tech-news-technology/how-digital-colonisation-is-still-keeping-internet-away-from-indian-languages-7057030/; Mishi Choudhary and Eben Moglen, "Head off Digital Colonialism: How Indian IT Can Compete with Google and Facebook and Show the World a Better Way," *Times of India*, May 28, 2017, https://timesofindia.indiatimes.com/blogs/toi-edit-page/head-off-digital-colonialism-how-indian-it-can-compete-with-google-and-facebook-and-show-the-world-a-better-way/.

18 "India's Data Must Be Controlled and Owned by Indians: Mukesh Ambani," *Mint*, December 19, 2018, https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyl/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html.

19 Amba Kak and Samm Sacks, "Shifting Narratives and Emergent Trends in Data-Governance Policy: Developments in China, India, and the EU," Yale Law School Paul Tsai China Center, August 2021, 5, https://law.yale.edu/sites/default/files/area/center/china/document/shifting_narratives.pdf.

20 "Report of the Joint Committee on the Personal Data Protection Bill," 10.

21 "Data Centre Policy 2020," Indian Ministry of Electronics and Information Technology, 2020, 3, https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf.

22 "Report of the Joint Committee on the Personal Data Protection Bill," 9.

critical of Modi and his party.[23] Legislators have also positioned data localization as international example setting. A memo attached to the 2019 draft of India's Personal Data Protection Bill described India as forging the fourth model of data governance—one designed for Global South countries, in contrast to the data models of China, the EU, and the United States. The Modi government echoed this view in 2019 when it refused to sign Japan's Data Free Flow with Trust agreement at the G20, later saying, "in view of the huge digital divide among countries, there is a need for policy space for developing countries."[24]

Currently, there is no single mechanism through which the US and Indian governments engage on cross-border data flow and data privacy issues. The United States and India have reconvened the Trade Policy Forum, which includes a sub-focus on digital and data matters, and they have an Information and Communications Technology (ICT) Working Group that convenes annually to promote ICT development and discuss cybersecurity, privacy, internet governance, and cross-border data flow issues—the former of which is only government, and the latter involves private-sector representatives.[25] Multiple government agencies and departments directly speak about and work on data policy, including the US Department of Justice and the Indian Ministry of Law and Justice, the US Department of State and the Indian Ministry of Foreign Affairs, and the US Department of Commerce and the Indian Ministry of Electronics and Information Technology. On top of this, both countries participate in multilateral forums on data and internet policy, standards, and norms, including the United Nations (UN) and the World Trade Organization (WTO). There are other forums in which the United States and other countries debate and develop data policy, like the Group of Seven (G7) and the Organisation for Economic Co-operation and Development (OECD), to which India is not a party.

This is not to suggest that this multipronged engagement is bad; on the contrary, funneling all bilateral communications related to cross-border data flows and data privacy—from MLAT requests around counterterrorism to trade disputes on data localization—would only bottleneck work on data issues. It also may not functionally make sense when groups as disparate as the US Department of Justice and the Indian Ministry of Electronics and Information Technology are involved in this issue set. However, this current setup still presents many challenges. There are multiple, relatively uncoordinated conversations occurring simultaneously about the same data policy topics. These conversations also tackle many of the same issues from different angles (e.g., law enforcement, trade, national security, and defense) and may, thus, do little to forge consensus among different US and Indian government stakeholders on the best approaches. The Indian government has also used the Personal Data Protection Bill dialogues as a reason to stall other data policy dialogues, whether in Indian courts or with foreign partners; for example, US trade officials have been forced to segment data localization and some other issues from primary US-India trade discussions, further stalling progress on US-India data policy.

Recommendations

The United States and India should convene bilateral dialogues, based in New Delhi, where US and Indian officials can discuss key cross-border data flow and data policy challenges. It is an open question how these dialogues should be situated vis-à-vis existing channels. The dialogues could be separate from the TPF and the ICT Working Group, because they would be an opportunity to focus on tangible, near-term, tactical objectives, rather than the higher-level strategic outcomes discussed in the TPF and the ICT Working Group. They could also be integrated into, or attached to, the reinvigorated TPF as a kind of high-priority issue area for the two countries, capitalizing on that process' momentum. At a minimum, this working group should only involve government officials from relevant diplomatic, law enforcement, and trade agencies and ministries—unlike the ICT Working Group, which involves the private sector.

23 See, e.g.: Nitish Pahwa, "Silicon Valley Thought India Was Its Future. Now Everything Has Changed," *Slate*, June 11, 2021, https://slate.com/technology/2021/06/india-silicon-valley-twitter-google-censorship.html.

24 Asit Ranjan Mishra, "India Says No to Free Flow of Digital Data at G20 Meeting," *Mint*, September 22, 2020, https://www.livemint.com/news/india/india-says-no-to-free-flow-of-digital-data-at-g20-meeting-11600787726265.html.

25 See, e.g.: Aditi Agrawal, "Indo-US ICT Working Group to meet on Sept 30, Oct 1," MediaNama, September 18, 2019, https://www.medianama.com/2019/09/223-indo-us-ict-working-group-to-meet-on-sept-30-oct-1; "Global Tech Association Urges Continued Bilateral U.S.-India Engagement on Eve of Annual ICT Working Group Meeting," Information Technology Industry Council, September 30, 2020, https://www.itic.org/news-events/news-releases/global-tech-association-urges-continued-bilateral-u-s-india-engagement-on-eve-of-annual-ict-working-group-meeting; "Joint Statement from the U.S.-India Information Communications Technology Working Group," US Embassy & Consulates in India, September 29, 2016, https://in.usembassy.gov/joint-statement-u-s-india-information-communications-technology-working-group/.

Washington and New Delhi are not going to arrive overnight, if ever, on the exact same page about data localization, digital sovereignty, and every other cross-border data flow and data privacy policy challenge. Many other issues—such as the United States pursuing a CLOUD Act agreement with India, and India pursuing adequacy agreements with the United States if the Personal Data Protection Bill is passed—are longer-term and more difficult challenges. Yet, there is still room for the United States and India to achieve tangible, near-term cooperation in some areas. The bilateral dialogues should focus on three of these areas with potential for near-term, tangible outcomes:

- **Law enforcement access to data.** These bilateral dialogues should discuss Indian law enforcement access to data, and how standardizing and better staffing data access requests could streamline the process. To be sure, the United States establishing a CLOUD Act agreement with India would help address issues with current MLAT data requests. It could also potentially better protect Indians' privacy and lessen Indian law enforcement's desire for data localization.[26] However, the US Department of Justice (DOJ) does not appear to have India at the top of the list for a CLOUD Act agreement, and drafting such an executive agreement could take much time and negotiation.[27] Thus, in the short term, the proposed US-India bilateral dialogues should address two of the main tensions in current Indian MLAT data access requests to the United States: the standardization of requests and the requisite staffing to process requests. First, on standardization, Indian law enforcement often files data access requests in different formats, so it takes more time for US companies or the US DOJ to log and process those requests. Both US companies and the US DOJ are also more likely to send back requests for additional information. Discussing how to address this problem—perhaps by the Indian government creating a standardized method and format of authoring and filing requests—could help resolve this bottleneck. It may even involve simpler solutions, such as Indian law enforcement offices using a single, known email address from which to send requests, which would make it faster than it currently is for companies to vet requests from unknown email (often, Gmail) accounts. Second, on requisite staffing, the US government is understaffed in processing Indian MLAT data access requests, and the Indian government is understaffed in dealing with requests for additional information. Investing more resources in staffing, especially on the US government side, would help streamline Indian law enforcement requests for data and streamline the US government response to those requests. These two efforts combined—depending on how much Indian law enforcement wants to access data the United States will not hand over—could also lessen law enforcement's incentives to push for data localization. This discussion could also serve as a sort of on-ramp for beginning to have conversations about future CLOUD Act agreement negotiations. That said, however, there is also an argument to be made that standardization will take much time and effort as well.

- **Definitions of and exceptions to data processing and localization requirements.** The bilateral dialogues should include discussion and early drafting of possible definitions of categories of which data may be subject to processing and localization requirements in the Personal Data Protection Bill, and a proposed list of exceptions. One of the largest gaps in the current draft is the definitions; many key terms are not clearly defined. For instance, the bill places different localization controls on "sensitive personal data" versus "critical personal data," but it defines the former very broadly and does not define the latter, saying the central government will decide. This creates uncertainty for industry, for Indian regulators responsible for enforcing data protection, and for US policymakers working on the CLOUD Act, MLAT requests, and related issues. This risks the central government coming up with arbitrary definitions (or amendments to them), or doing so through a highly politicized process. It also suggests that parliament has not yet established the exact scope and shape of proposed data storage, processing, and transfer requirements. The broad requirements for companies to hand over "non-personal data" to the government are also concerning, and demand further discussion. Thus, the bilateral dialogues should tackle these definitional issues and propose language in response. The participants should also discuss and begin drafting a list of proposed exceptions to the bill's processing and localization requirements. The bill concerningly exempts

26 Madhulika Srikumar, "The Privacy Negotiators: The Need for U.S. Tech Companies to Mediate Agreements on Government Access to Data in India," New America, August 2019, https://www.newamerica.org/fellows/reports/anthology-working-papers-new-americas-us-india-fellows/the-privacy-negotiators-the-need-for-us-tech-companies-to-mediate-agreements-on-government-access-to-data-in-india-madhulika-srikumar/.

27 Peter Swire, DeBrae Kennedy-Mayo, and Arjun Jayakumar, "India's Access to Criminal Evidence in the U.S.: A Proposed Framework for an Executive Agreement," Observer Research Foundation, December 2020, https://www.orfonline.org/research/indias-access-to-criminal-evidence-in-the-us/.

the Indian government from many of the bill's privacy controls, and it has some detail about other exemptions (e.g., for research, for small entities processing data manually) but not much. Bilateral discussions could help shape these rules in a mutually beneficial fashion, while also lending insight into how Indian regulators might enforce the bill in practice. How these exceptions are written and enforced will impact everything from Indians' privacy to scientific research, healthcare data analysis, and the competitiveness of US and Indian companies—and it is critical for the exceptions to be written carefully, and with stakeholder input.

- **Cybersecurity of data.** The bilateral dialogues should include discussion of the impacts of proposed cross-border data policies, including data localization, on cybersecurity—and what cybersecurity steps must be taken in response. Protecting citizens' information is vital for individual privacy, business operations and competitiveness, and national security. The United States and India, therefore, have a strong interest in ensuring that data stored on Indian citizens and data stored in India are protected from criminals, foreign states, and other hackers. As the Joint Parliamentary Committee report notes, "the role of data security is fundamental," and "when a data protection ecosystem is being pursued, it must be noted that appropriate data security should take into account the requirements of individual data subjects, controllers and personal data itself."[28] The Centre for Information Policy Leadership (a think tank) and the Data Security Council of India (an industry body) likewise noted in a report that considerations of data localization rules must also weigh the potential impacts on cybersecurity.[29] Data localization, for instance, may prevent information sharing between India and other countries on how to respond to new and severe cyber threats. Requirements to store and process data in local data centers can also end up undermining individual privacy, business competitiveness, and national security if those requirements do not mandate strong cybersecurity protections, and if the local architecture has weaker cybersecurity than where the data might otherwise be stored. The bilateral dialogues should address the cybersecurity implications of the Personal Data Protection Bill and other proposed US and Indian data policies—and come up with a list of near-term, tactical responses to address the cybersecurity risks.

Conclusion

Now that Washington and New Delhi have kicked back off the TPF, both countries have a renewed opportunity to tackle head on some of the most challenging and important issues in US-India cross-border data flows and data policy. Principally, this should be done through bilateral dialogues, based in New Delhi, that focus on tactical, low-hanging-fruit objectives, rather than high-level strategic dialogue: law enforcement access to data; definitions of, and exceptions to, data processing and localization requirements; and cybersecurity of data. Few are under any illusion that the United States and India will arrive overnight, if ever, on the exact same page about major questions of cross-border data flows, data privacy, and the notion of sovereignty in the digital age. Yet, with major issues of individual privacy, economic growth and competitiveness, and even national security in the balance, the United States and India should pursue what cooperation they can on these critical cross-border data flow and data policy challenges.

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, where his work focuses on the geopolitics, governance, and security of the global internet. He is also a research fellow at the Tech, Law & Security Program at American University Washington College of Law, a fellow at Duke University's Sanford School of Public Policy, and a contributor at *WIRED* Magazine. He chaired the Cross-Border Data Flows and Data Privacy Working Group for the Atlantic Council's Initiative on US-India Digital Trade.

28 "Report of the Joint Committee on the Personal Data Protection Bill," 8.

29 "Enabling Accountable Data Transfers from India to the United States Under India's Proposed Personal Data Protection Bill (No. 373 of 2019)," Centre for Information Policy Leadership and Data Security Council of India (Noida: Data Security Council of India, August 2020, 8, https://www.dsci.in/sites/default/files/documents/resource_centre/DSCI-CIPL-Accountable-Data-Transfer-Report.pdf.

Acknowledgments

The author would like to thank all the members of the Cross-Border Data Flows and Data Privacy Working Group, of the Atlantic Council's Initiative on US-India Digital Trade, for their time and expertise in multiple Chatham House Rule discussions about these issues. The author would also like to thank Peter Swire, DeBrae Kennedy-Mayo, Madhulika Srikumar, Mark Linscott, Anand Raghuraman, Atman Trivedi, and Katherine Hadda for feedback on an earlier draft of this issue brief. Finally, the author would like to thank Irfan Nooruddin, Capucine Querenet, and the rest of the Atlantic Council's South Asia Center for their support. The author's views are their own and do not necessarily reflect those of the working group participants, whose names shall remain anonymous.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

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

TREASURER
*George Lund

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

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
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 February 15, 2022

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