

Article

The United States and India: A Digital Partnership in Need of a Strategy

Arjun Kang Joseph and Rudra Chaudhuri

Abstract

India-US relations have transformed in the last two decades. The defence and strategic partnership remains the silver-lining in an equation increasingly shaped by the rise and bellicosity of China. Yet, there is another aspect of this relationship that has been largely neglected: the need to bridge growing divergences in each countries' approach to the digital economy. This paper outlines these divergences and suggests ways forward. It makes the case that the differences, at the tactical level, requires an investment at the strategic level to make the best of the future of digital ties. In particular, the paper lays down the reasoning to invest in what might be called the Next Steps in Technological Partnerships, just like India and the United States invested in the Next Steps in Strategic Partnership more than a decade ago. The latter had a telling impact on the growth of India-US defence ties. There is no reason why the former cannot have the same effect as far as digital ties are concerned.

The relationship between the United States and India has transformed over the last two decades. The defence relationship grows in breadth and depth every year. Even the administration of President Donald J. Trump, which paid scant attention to its formal allies, “acted with uncharacteristic diligence”—as a former Senior Director in the United States National Security Council argues— “to advance cooperation on a range of security issues.”¹ By the end of the Trump administration, the last foundational defence agreement was signed between the two countries.² Yet, as far as trade and commerce is concerned, the results have been far from fruitful. A narrow trade agreement, negotiated for over two

Arjun Kang Joseph is a research analyst with the Technology and Society Program at the Carnegie India. His research focuses on data, privacy and the intersection of health and technology. Rudra Chaudhuri is the director of Carnegie India. His primary research interests include the diplomatic history of South Asia and contemporary security issues.

years, came to knot. Sharp differences in views over intellectual property rights, market access—especially in pharmaceuticals and agricultural products, and the digital economy have led to a breakdown in talks.

How the incoming Biden administration seeks to approach—and perhaps revive—the trade relationship is yet to be seen. What is clear is that for the Joe Biden Presidency, securing supply chains and focussing on domestic economic revival will be a priority. An Executive Order by the U.S. President underlines: “resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America’s competitive edge in research and development, and create well-paying jobs.”³ The objective will be to find the right balance between globalism and domestic economic renewal.⁴ In short, a more global Biden presidency may be a lot less forgiving when it comes to trade agreements. Moreover, both the United States and India will need to bridge the growing divide when it comes to the digital economy. Currently, data is “not on the formal trade stack” in dialogue between the two countries, though it is a major area of dispute.⁵

...India is an attractive market for American companies from Facebook and Google to Microsoft and Intel.

To be sure, India is an attractive market for American companies from Facebook and Google to Microsoft and Intel. It is the largest open data market in the world. More than a billion Indians will have access to a smart phone by 2024. Close to 600 million Indians already use 4G data. Per capita, more data is consumed in India than anywhere in the world. This is facilitated by the low data rates available in the country.⁶ For the development and future of emerging technologies, such as artificial intelligence and blockchain, India’s data market is of crucial importance.

American companies invested in India contribute to its economic growth. American capital and venture capitalists play an important role in providing buoyancy to India’s much admired start-up economy. The suburbs of Bengaluru, Hyderabad, and the centre of Gurugram are testament to the connection between Silicon Valley and the frontiers of India’s tech-economies. This is a partnership that has grown organically over the last two decades. Its chief facilitators include global citizens, who have spent time and invested in these dual geographies. Communities of these netizens, across continents, have helped forge a partnership that has thrived outside of government. Officials at the highest levels are required to close defence agreements. Tech entrepreneurs—armed with H1B visas and the drive to succeed—have laid the foundations of the laissez faire digital partnership between the world’s two largest democracies.

Yet, this partnership is now in need of a strategy. It requires an official intervention. The differences over the treatment and access to data are too sharp for netizens. To truly realise the potential in the U.S.-India relationship, it is crucial to invest in a strategic dialogue that addresses the growing differences in the digital economy. The aim of this article is to outline the differences between the two countries. First, on data localisation, i.e., the practice of limiting data storage to the country. Second, on data access and how the two countries grant access to data to law enforcement agencies. The article does not deal with the sharp difference in e-commerce policies, this is well covered in existing analyses.⁷ It concludes by providing a brief account of how the Indian government and the Biden administration could start to think collectively and much more strategically about the future of their digital relationship.

The Localisation Challenge

“Localisation is going to slow-down the evolution of growth in the Indian economy,”⁸ is how a senior American diplomat in the Trump administration put it. No doubt, the extent to which India chooses to localise data will have significant effects on the trade and the larger bilateral relationship with the United States. Localisation is not new in, and to, India. All telecom data is localised in India. Financial data is localised, much to the chagrin of companies like Visa and Mastercard.⁹

In essence, data localisation is a policy measure that restricts the flow of data across geographical and jurisdictional boundaries. There are four primary reasons for countries to restrict the flow of data. First, because of the risk of personal data being misused. Second, because of the difficulties of accessing personal data, often stored on servers outside of that country. Third, because the data might be at risk of being under surveillance by foreign intelligence agencies. Fourth, because of a potential economic loss to the country. This is how an expert committee in India—under the Chairmanship of Justice Srikrishna—interpreted the rationale for localising data.¹⁰

In India, localisation requirements are embedded in a range of notifications. A draft Personal Data Protection Bill (PDPB)—a version of which is currently being examined by a Joint Parliamentary Committee (JPC),¹¹ a Reserve Bank of India notification on ‘Storage and Payment System Data’,¹² the draft National e-Commerce Policy,¹³ and the Draft E-Pharmacy Regulations,¹⁴ for example, contain some form of localisation requirement.

The most important of these regulations is the draft PDPB. When it becomes a law, potentially in 2021, it will set-out the architecture of a cross-sectoral requirement for localisation. Following two rounds of stakeholder consultations, a transformed Personal

Data Protection Bill, 2019 was tabled in the Lok Sabha in December, 2019.¹⁵ This version of the Bill relaxed the localisation requirement by allowing the transfer of personal data outside of India's borders, but it still required the local storage of sensitive personal data, though transfer for the purpose of processing is allowed with explicit consent and subject to certain conditions; and critical personal data for which storage and processing must only be done in India.¹⁶ The Bill is being examined by a Joint Parliamentary Committee (JPC).¹⁷ There is every likelihood that the Bill, and ultimately the law, will contain certain localisation requirements.

The United States, on the other hand, only requires critical information for operational security or defence data to be stored.¹⁸ In the 2019 National Trade Estimate, the Office of the United States Trade Representative cited data flow restrictions as "key barriers to trade" and noted—"When governments impose unnecessary barriers to cross-border data flows or discriminate against foreign digital services, local firms are often hurt the most, as they cannot take advantage of cross-border digital services that facilitate global competitiveness."¹⁹ This divergence in the approach to data regulation has clearly strained U.S.-India relations. It is for this reason that an investment in a strategic dialogue on technology is essential.

In the last two years of the Trump administration, both Indian and American representatives found it impossible to enter into a slim trade agreement. This clarified the United States' hard-nosed position on the free flow of data. Reportedly, American officials even considered caps on H-1B work visas for nations that forced the implementation of localisation. This was particularly concerning for India, which is estimated to account for 70 percent of the 85000 H-1B work visas granted each year.²⁰ Prior to this, the then United States Secretary of State Mike Pompeo had stated—"We will also push for free flow of data across borders, not just to help American companies, but to protect data and secure consumers' privacy." The State Department later clarified that it had no plans to place such caps on H-1B work visas.²¹ Yet, that data localisation is a matter of strategic concern for the United States, is now clear. After all, the business models of most American technology companies functioning in India are premised on the free flow of data across borders. On the other hand, what is also clear is that the expected economic gains of localisation have been overestimated. Further, the popular conceptualisation of data as a natural resource is inherently misleading.²²

To be sure, the disagreements over the localisation of data are not only a bilateral matter between the United States and India. There is an increasing global effort to consider international data governance. Here too, the United States and India find each other on

opposite sides of the debate. In April 2019, Japanese Prime Minister Shinzo Abe outlined the contours of what came to be known as the 'Osaka Track' at the G20 leaders' summit.²³ The Osaka Track set the stage for plurilateral negotiations on digital trade. The aim is to enable data flows and strike down barriers to those flows. In time, these efforts came to be enshrined in a charter known as the Data Free Flow with Trust (DFFT). For excellent reasons, India boycotted the Osaka Track.²⁴ In September 2020, the minister of commerce and industry—Piyush Goyal—made clear that India was not in a position to sign onto the DFFT. After all, how could India sign onto an international norm setting agreement, without first passing the PDPB? Moreover, the minister made clear that 'equitable access' to data is central to India's concerns.²⁵

Yet, once India does pass the PDPB, and hence will have, through legislation, a policy in place for the protection and movement of personal data, it will need to carefully consider how best to deal with data diplomacy with its key strategic and trading partners. Indeed, it is increasingly clear that the objectives that India seeks to accomplish via localisation, as outlined above, can in fact be achieved through alternative means without necessarily localising data.²⁶ Searching for these alternatives becomes all the more important when we consider the risk of retaliatory action by other nations, as well as the risk of reduced Foreign Direct Investment due to increased compliance costs and a reduction in ease of doing business. Additionally, this approach does not consider the potential benefits arising from the data flows.²⁷ Whatever the Indian government's final decision will be on localisation, investing in a strategic dialogue with the United States could be beneficial for both countries, as they chart the future course of data diplomacy. Further, using this strategic track to consider the frictions arising out of data access issues will be equally important.

Data Access between India and the US

Between January and June 2020, Google²⁸ and Facebook²⁹ received a total of 46,745 requests from Indian law enforcement authorities asking for access to 84,902 users or accounts information. The two companies produced data in response to 58% and 50% of these requests, respectively. In the same period, Twitter's requests from India increased by 254%, while the number of accounts specified increased by 69%.³⁰ A combination of the time taken, and low success rates has been the cause of ever-growing frustration for Indian law enforcement agencies. Indeed, Indian law and enforcement officials from the police to the National Investigative Agency (NIA) make clear that the difficulties in accessing data held by foreign companies functioning in India is a major point of friction. Partially, for these reasons, the Indian government recently announced the 'Intermediary Guidelines and Digital Ethics Code' 2021.³¹ The new rules have been read by analysts as a way by which the

government can force technology companies to break encryption with the view to access data.³² The latest regulations are bound to lead to an even higher degree of conflict between security agencies in India and technology companies—many of which are American—in the near future.

These tactical level issues—if one can call them that—have clearly spilled onto the strategic relationship between the two countries. These are matters of considerable debate in bilateral meetings between law and enforcement agencies in both countries. It is not for nothing that the incoming Biden administration in the United States sees technology and the many debates therein as a critical feature of its approach to world politics. Technology alliances,³³ and AI-led partnerships are going to be of critical concern for this administration.³⁴ Finding a mutual solution to issues around data access should be a step towards building a strategic technology partnership with the United States.

Currently, Indian data access requests are made through MLATs (mutual legal assistance treaties) or Letters Rogatory. This system is criticized for being slow, cumbersome, and lacking sufficient data protection safeguards.³⁵ A 2013 U.S. official report found that the time from start to finish for the MLAT process is an estimated average of at

Finding a mutual solution to issues around data access should be a step towards building a strategic technology partnership with the United States.

least 10 months.³⁶ Law and enforcement agencies in India are tired of using this mechanism for accessing data. Indeed, some estimates from Indian sources say it can take 40 months on average to access data that is held on servers outside of India's borders.³⁷ The Letters Rogatory process enables a court to issue letters of request to a foreign court or authority for the production of a document.³⁸ It is however important to

note that recipients of Letters Rogatory requests are under no treaty obligation to process them. This system functions on reciprocity.

This has led to data access issues being one of the driving forces for data localization in India. This policy measure, however, overlooks the fact that the physical storage of data in India will not lead to improved data access unless a new policy framework for the same is created. Rather than focusing on the physical location of the data, it would be in India's merit to consider solutions that get to where the data is. Which would be to move the law to the data and not the data to the law.³⁹

Cross-border data access requests are governed by the laws of two countries. The country from where the request is made and the country where the entity receiving

the request is based or where their data is stored. Indian laws on government data access are criticized for lacking oversight, being overly broad in terms of the scope and powers, and silent on necessary restrictions and limitations. The exemptions for law enforcement agencies under the Personal Data Protection Bill, 2019 are also a cause for concern for many countries.⁴⁰

The United States' Stored Communications Act, bars entities within its jurisdiction from sharing the contents of stored communications, except in accordance with the provisions of that law.⁴¹ Other countries can gain access to this data through a court order passed in the United States through MLATs or Letters Rogatory. These entities are also permitted to share non-content related records or other information with foreign agencies on a voluntary basis.⁴²

In March 2018, the United States enacted the CLOUD (Clarifying Lawful Overseas Use of Data) Act to facilitate data access. The Act allows the United States to enter into executive agreements that will improve data access from U.S. based providers by foreign partners.⁴³ Under the Act, these executive agreements can only be made when: (a) the U.S. attorney general, in concurrence with the Secretary of State, determines that the country's overall legal and procedural framework satisfies certain conditions (protection of privacy and civil rights, adherence to rule of law and international human rights obligations, commitment to the global free flow of data, etc.), and (b) certain conditions are met with regard to the purpose of requests, reasonable justification for the request and judicial review and oversight. As it stands, India cannot enter into an executive agreement with the U.S. under the CLOUD Act. Many of India's laws and practices are incompatible with conditions provided in the Act. The legal and procedural safeguards under Indian law fall short of the requirements of the Act.⁴⁴

India and the U.S. have already made some efforts to reform the MLAT process. The two countries should pursue further renegotiation and reform to increase the efficiency of these existing processes. Additionally, India has several routes it could take going forward. It could come together with other countries to create a new multilateral framework to regulate trans-border access to personal data. It could reconsider being a party to the Budapest Convention—a multilateral framework to deal with data access—or signing an amended executive agreement under the CLOUD Act or prepare its own model agreement for data access.⁴⁵ Regardless of what choice it makes, it is necessary to engage with partners in the United States more actively to find a solution with regards to the access of data.

Conclusion: The need for strategy

'We have to push back against the Chinese government's economic abuses and coercion,' argued President Joe Biden at the 2021 Virtual Munich Security Conference. The aim, he underlined, was that "everyone must play by the same rules."⁴⁶ Yet, what these new rules are, and who will ultimately shape them, remains unclear. Biden's commitment to America's allies and the North Atlantic Treaty Organisation is abundantly clear. As he highlighted in his Munich speech, "the transatlantic alliance is back." As far as technology is concerned, finding common ground between the United States and Europe will prove hard. European partners are unwilling to cut out Chinese investments in 5G.⁴⁷ There is a raging debate between the two continents on privacy standards, including on surveillance, that have blocked, for now, the free movement of data between the two jurisdictions.⁴⁸

These are warning signs for New Delhi. If the United States and Europe find it difficult to bridge differences on the future of technology, it is going to be anything but an easy task between the U.S. and India. As mentioned above, tactical issues like localisation and data access have, already, strained the relationship. There is an urgent need to institute a strategic process by which differences and convergences on technology are given the same importance as both countries placed on defence ties more than a decade and a half ago. It is worth recollecting that the Next Steps in Strategic Partnership (NSSP),⁴⁹ in 2005, paved the way for the completion of the U.S.-India Nuclear Deal in 2008. It also led to the marked increase in the defence relationship between the two countries. The 'foundational agreements' discussed in the introduction to this chapter would have been impossible without the NSSP. In short, strategic thinking drove the defence and geopolitical aspects of this relationship. It is high time that similar strategic approaches are adopted with regards to technology.

Recommendations

To start with, the U.S.-India Information and Communication Technology (ICT) Working Group could be upgraded. It was 'revived' in 2015 with little effect.⁵⁰ Further, a new strategic track, something along the lines of a Next Steps in Technological Partnerships (NSTP) ought to be considered and led on each side by a top official—at the level of a Secretary—from the United States and from India. In fact, much like the 2+2 process, which includes foreign affairs and defence, the NSTP should provide space for a 3+3 process: which would include the Secretaries from the Ministry of External Affairs, the Ministry of Electronics, and Information Technology, and at least one deputy National Security Advisor. To be sure, data is not just a domestic and economic matter of debate. It is of strategic

concern. How India—first on its own, and then with the United States—approaches the use of, and access to, data could set the tone for international negotiations on the same at the G20, the WTO, and elsewhere.

Lastly, a 3+3 could, and should, consider areas of technological convergences in the long term. This is not a forum that should be hypnotised by immediacy. There is much to be discussed and collaborations to be built in the worlds of ETs, from the future of quantum computing to the Internet of Things. India remains the largest open data market in the world. Hence, structurally, this is a market that cannot be ignored. However, it is imperative to fully appreciate that the future of technology lies in collaboration and partnerships. If India truly wants to shape the technological debates and norms that shape the future of data diplomacy, it is important to work, first, with those that it has invested so much in. The United States is such a partner. It has capital whilst India has scale. Both share a similar zeal for innovation.

What is needed, more immediately, is an equal investment in a strategic approach to arrest the tactical level frictions arising out of localisation and the issues around the access to data. The aim should be to capitalise on the endless possibilities in the future of emerging technologies to solve for some of the most pressing challenges of our times, from shortages in water to better results in agriculture. For this to happen, the U.S.-India relationship needs an investment in strategizing the future of technology, which, at present, is absent.

References

1. White, Joshua T. "After The Foundational Agreements: An Agenda For US-India Defense And Security Cooperation." Brookings. January 2021. https://www.brookings.edu/wp-content/uploads/2021/01/FP_20210111_us_india_white.pdf.
2. Roy, Shubhajit. "Explained: BECA, and the Importance of 3 Foundational Pacts of India-US Defence Cooperation." The Indian Express. November 03, 2020. <https://indianexpress.com/article/explained/beca-india-us-trade-agreements-rajnath-singh-mike-pompeo-6906637/>.
3. "Executive Order on America's Supply Chains." The White House. February 24, 2021. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>.
4. Salman Ahmed, Karan Bhatia. "U.S. Foreign Policy for the Middle Class: Perspectives From Ohio." Carnegie Endowment for International Peace. <https://carnegieendowment.org/2018/12/10/u.s.-foreign-policy-for-middle-class-perspectives-from-ohio-pub-77779>.
5. Interview with a senior American official, February 2020. Both US and India needs to bridge the growing divide on digital economy because presently the data is "not on the formal

trade stack” in dialogue between the two countries, though it is a major area of dispute.

6. Chaudhuri, Rudra. “India’s Path Ahead: On India’s Role in Technology Standards - The Day After.” Carnegie Endowment for International Peace. September 09, 2020. <https://carnegieendowment.org/2020/09/09/on-india-s-role-in-technology-standards-pub-82496>.
7. Mukherjee, Arpita, and Avantika Kapoor. “Trade Rules in E-commerce: WTO and India.” ICRIER. March 2018. https://icrier.org/pdf/Working_Paper_354.pdf.
8. Carnegie India’s Closed-door discussion on Technology, Data and the Future of US-India Relations, Global Technology Summit, December 2020. “Localisation is going to slow-down the evolution of growth in the Indian economy,” is how a senior American diplomat in the Trump administration put it.
9. Gupta, Komal. “Visa, Mastercard Begin Storing India Payments Data Locally.” Mint. October 30, 2018. <https://www.livemint.com/Industry/Wmq7Sr5YtNBPcet8aGBRQP/Visa-Mastercard-begin-storing-India-payments-data-locally.html>.
10. “A Free and Fair Digital Economy Protecting Privacy, Empowering Indians: Committee of Experts under the Chairmanship of Justice B.N. Srikrishna.” MeitY. July 27, 2018. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.
11. “The Personal Data Protection Bill, 2018.” MeitY. https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
12. “Storage of Payment System Data.” RBI. April 6, 2018. <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF>.
13. “Draft National E-Commerce Policy: India’s Data for India’s Development.” Department For Promotion of Industry and Internal Trade. https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.
14. Ministry of Health And Family Welfare (Department of Health and Family Welfare). “Notification: Amendment to the Drugs and Cosmetics Rules (1945)”. 28 August 2018. https://cdsco.gov.in/opencms/opencms/system/modules/CDSCO.WEB/elements/download_file_division.jsp?num_id=MTkzOQ==
15. “The Personal Data Protection Bill, 2019.” PRS India. December 11, 2019. <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019>.
16. “The Personal Data Protection Bill, 2019.” http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
17. Agarwal, Surabhi. “89 Amendments, 1 New Clause in Final Draft of India Data Protection Bill.” The Economic Times. January 07, 2021. <https://economictimes.indiatimes.com/tech/technology/89-amendments-1-new-clause-in-final-draft-of-india-data-protection-bill/articleshow/80144191.cms?from=mdr>.

18. "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-Do18)." Federal Register. August 26, 2015. <https://www.federalregister.gov/documents/2015/08/26/2015-20870/defensefederal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for#sectno-reference239.7602-2>.
19. "Fact Sheet On The 2020 National Trade Estimate: Strong, Binding Rules to Advance Digital Trade." United States Trade Representative. <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2020/march/fact-sheet-2020-national-trade-estimate-strong-binding-rules-advance-digital-trade>.
20. Dasgupta, Neha, and Aditya Kalra. "Exclusive: U.S. Tells India It Is Mulling Caps on H-1B Visas to Deter Data Rules - Sources." Reuters. June 19, 2019. <https://www.reuters.com/article/us-usa-trade-india-exclusive-idUSKCN1TK2LG>.
21. Lakshman, Sriram. "No H1B Visa Caps in Retaliation for Data Localisation: U.S. State Department." The Hindu. June 21, 2019. <https://www.thehindu.com/news/international/no-h1b-visa-caps-over-data-localisation-us-state-department/article28093898.ece>.
22. Kathuria, Rajat, Mansi Kedia, Gangesh Varma, and Kaushambi Bagchi. "Economic Implications of Crossborder Data Flows." ICRIER. November 2019. https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf.
23. "G20 OSAKA SUMMIT (Summary Of Outcome)." Ministry of Foreign Affairs of Japan. June 29, 2019. https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/overview/.
24. Kanth, D. Ravi. "India Boycotts 'Osaka Track' at G20 Summit." Mint. June 30, 2019. <https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html>.
25. PTI. "India Not in a Position to Accept Concept of DFFT, Says Piyush Goyal." Business Standard. September 22, 2020. https://www.business-standard.com/article/economy-policy/india-not-in-a-position-to-accept-concept-of-dfft-says-piyush-goyal-120092201651_1.html.
26. Basu, Arindrajit, Elonnai Hickok, and Aditya Singh Chawla. "The Localisation Gambit Unpacking Policy Measures for Sovereign Control of Data in India." Centre for Internet and Society. March 19, 2019. <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>.
27. Kathuria, Rajat, Mansi Kedia, Gangesh Varma, and Kaushambi Bagchi. "Economic Implications of Crossborder Data Flows." ICRIER. November 2019. https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf.

28. "Global Requests for User Information." Google Transparency Report. https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:IN.
29. "Facebook Transparency Report: Gov Data Requests." Facebook Transparency. <https://transparency.facebook.com/government-data-requests/country/IN>.
30. "Removal Requests - Twitter Transparency Center." Twitter. <https://transparency.twitter.com/en/reports/removal-requests.html#2020-jan-jun>.
31. "Notification Dated, the 25th February, 2021 G.S.R. 139(E): The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Ministry of Electronics and Information Technology, Government of India." MeitY. February 25, 2021. Accessed March 11, 2021. <https://www.meity.gov.in/content/notification-dated-25th-february-2021-gsr-139e-information-technology-intermediary>.
32. Raghavan, Malavika. "For More Online Civility, We Will Need Deeper Engagement, Careful Legislation." The Indian Express. March 01, 2021. <https://indianexpress.com/article/opinion/columns/social-media-ott-rules-india-digital-content-publishers-7208935/>.
33. Bradford, Anu, and Raluca Csernaton. "Toward a Strengthened Transatlantic Technology Alliance - Working With the Biden Administration: Opportunities for the EU." Carnegie Endowment for International Peace. January 26, 2021. <https://carnegieendowment.org/2021/01/26/toward-strengthened-transatlantic-technology-alliance-pub-83565>.
34. PTI. "US Body on AI Calls for Creating India-US Strategic Tech Alliance." Business Standard. October 14, 2020. https://www.business-standard.com/article/international/us-body-on-ai-calls-for-creating-india-us-strategic-tech-alliance-120101400733_1.html.
35. Srikumar, Madhulika et al. "India-US Data Sharing for Law Enforcement: Blueprint for Reforms." ORF. January 17, 2019. https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.
36. "Liberty And Security In A Changing World." Obama White House. December 12, 2013. https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
37. Alawadhi, Neha. "CBI & FBI Join Hands to Reduce Time Required to Fulfil Requests on Information and Evidence." The Economic Times. December 06, 2015. <https://economictimes.indiatimes.com/news/politics-and-nation/cbi-fbi-join-hands-to-reduce-time-required-to-fulfil-requests-on-information-and-evidence/articleshow/50069794.cms>.
38. "Comprehensive Guidelines for Investigation Abroad and Issue of Letters Rogatory." Ministry of Home Affairs. December 31, 2007. <https://www.mha.gov.in/sites/default/files/LR-170709.pdf>.

39. "Notification Dated, the 25th February, 2021 G.S.R. 139(E): The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Ministry of Electronics and Information Technology, Government of India." MeitY. February 25, 2021. Accessed March 11, 2021. <https://www.meity.gov.in/content/notification-dated-25th-february-2021-gsr-139e-information-technology-intermediary>.
40. Smriti Parsheera, Prateek Jha. "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?" Carnegie India. November 23, 2020. <https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197>.
41. "18 United States Code (U.S.C.) § 2702 and 2703." U.S.C. Title 18 - CRIMES AND CRIMINAL PROCEDURE. <https://www.govinfo.gov/content/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm>.
42. "U.S.C. Title 18 - CRIMES AND CRIMINAL PROCEDURE." Govinfo.gov. <https://www.govinfo.gov/content/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm>
43. "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act." April 2019. <https://www.justice.gov/opa/press-release/file/1153446/download>.
44. Hickok, Elonnai, and Vipul Kharbanda. "An Analysis of the CLOUD Act and Implications for India." The Centre for Internet and Society. August 22, 2018. <https://cis-india.org/internet-governance/files/analysis-of-cloud-act-and-implications-for-india>.
45. Smriti Parsheera, Prateek Jha. "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?" Carnegie India. November 23, 2020. <https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197>.
46. "Remarks by President Biden at the 2021 Virtual Munich Security Conference." The White House. February 19, 2021. <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/19/remarks-by-president-biden-at-the-2021-virtual-munich-security-conference/>.
47. Sevastopulo, Demetri. "US vs China: Biden Bets on Alliances to Push Back against Beijing." Financial Times. March 04, 2021. <https://www.ft.com/content/cf71feb2-297f-4e3a-8627-b89931cc6a80>.
48. Meltzer, Joshua P. "Why Schrems II Requires US-EU Agreement on Surveillance and Privacy." Brookings. December 08, 2020. <https://www.brookings.edu/techstream/why-schrems-ii-requires-us-eu-agreement-on-surveillance-and-privacy/>.

49. "India and United States Successfully Complete Next Steps in Strategic Partnership." Ministry of External Affairs, Government of India. July 18, 2005. [https://www.mea.gov.in/bilateral-documents.htm?dtl/6789/India and United States Successfully Complete Next Steps in Strategic Partnership](https://www.mea.gov.in/bilateral-documents.htm?dtl/6789/India%20and%20United%20States%20Successfully%20Complete%20Next%20Steps%20in%20Strategic%20Partnership).
50. Jain, Rahul. "Revival of India-US ICT Working Group: Significance for India." ORF. March 16, 2015. <https://www.orfonline.org/research/revival-of-india-us-ict-working-group-significance-for-india/>.