CROSS-BORDER DATA FLOWS & FREE TRADE AGREEMENTS

WHAT ARE CROSS-BORDER DATA FLOWS?

The phrase "cross-border data flows" refers to the movement or transfer of digital information between servers located in different countries.

The growth of the digital economy over the last few decades has seen an increase in the amount of data being collected from consumers of various digital services. This data is not always stored within the country where the consumer is located. Often, the data is moved around the world by technology companies who process this data to derive their profits.

The cross-border transfer of information, while beneficial to technology companies (who can store data in cheaper locations or in jurisdictions that allow relatively unregulated processing of the data) can leave consumers at risk of having their privacy rights infringed. As noted by the OECD, "the ubiquitous exchange of data across borders has amplified a range of concerns for governments, businesses and citizens, eroding trust among them."[1] In response, many countries are adopting measures to regulate cross-border flows of data, often placing restrictions on how data is shared and when it can be transferred abroad.[2]

WHY REGULATE CROSS-BORDER DATA FLOWS?

There are different reasons why countries may seek to regulate cross-border data transfers, though these may broadly be categorized under the following justifications:

I. **To protect civil liberties:** Restricting foreign data transfers can ensure that domestic data protection, privacy, and cyber security law can be applied to the data. In addition to enforcement of law, ensuring data remains within a country can also ease audit and supervisory processes.

DIGITAL TRADE ALLIANCE

II. **To ensure that data is accessible:** Local law enforcement and regulatory authorities must be able to access data to perform their regulatory and supervisory functions and ensure national security in terms of protecting particularly sensitive information.

III. **For economic reasons:** For example, policymakers may seek to develop local capacity in the digital sector.

Regulations on cross-border data flows can take a variety of forms, including restrictions on the export of data altogether, requirements to maintain a local copy of data, requirements to obtain consent before a transfer to a third country, or even taxes on data exports.[3]

While a number of countries (including China, Russia, and Vietnam) implement fairly broad restrictions on cross-border data transfers, many countries implement sectoral restrictions based on the perceived sensitivity of the data and the risk posed by misuse thereof. Thus, several countries (including Australia, Germany, India, Indonesia and South Korea), implement restrictions on cross-border transfers of health data, financial data, telecommunications-related data, government data, etc.

WHY IS THIS ISSUE IMPORTANT?

The digital economy to a large extent relies on the commodification of personal data to derive its profits. At the same time, consumers are increasingly seeking to control their personal data. Scandals such as Cambridge Analytica, with the invasive and constant tracking and exploitation of people's data, have eroded people's trust in cross-border data transfers.[4] Multiple studies reveal that a large majority of consumers around the world are concerned about the collection of their personal data online by companies.[5]

When data moves across borders, it is subject to a different legal regime. This can be problematic if the foreign jurisdiction offers comparatively limited or no privacy rights to consumers. Companies can therefore evade local privacy and data protection norms merely by moving data to a different location, putting consumer rights at risk.

Accordingly, a number of governments have implemented regulations to provide consumer rights over data and to ensure data is adequately protected irrespective of its location. For instance, the European Union's General Data Protection Regulation (GDPR), seen as a gold standard for data protection law, implements various conditions that seek to ensure that personal data will be securely processed even if transferred to a foreign jurisdiction.[6]

However, such measures could be susceptible to challenge under some recent free trade agreements (FTAs) that contain provisions limiting the ability of states to implement any restrictions/encumbrances on cross-border data transfers. Notably, provisions liberalizing

international data flows treat privacy and data protection regulations as trade barriers, thereby enabling cross-border data transfers without regard for rules that guarantee minimum data protection standards.

WHAT DO FTAS SAY ABOUT CROSS BORDER DATA FLOWS?

In general, Big Tech companies have championed international obligations that limit governments' abilities to restrict cross-border data flows. These attempts have been resisted by others, including on account of the need to ensure adequate privacy protection to data outside its home jurisdiction.

While initial attempts to discuss these issues under the rubric of the World Trade Organisation (WTO) have stalled, a separate negotiating track known as the Joint Statement Initiative on ECommerce (JSI) was launched in 2017 to reach agreement on digital trade-related issues. However, there continues to be significant divergence about how to treat cross-border data flows even at this forum.[7]

In the absence of any agreement at the WTO, discussions related to cross-border data transfers were included in other multilateral arrangements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Regional Comprehensive Economic Partnership (RCEP), the United States-Mexico-Canada Free Trade Agreement (USMCA), and the Osaka Track launched at the G20 discussions in Japan in 2019.

One of the first big trade agreements to include provisions concerning cross-border data flows was the Trans-Pacific Partnership Agreement, which evolved into the CPTPP following the withdrawal of the United States. Article 14.11 of the CPTPP requires parties to allow cross-border transfers of data. This requirement is, however, subject to: (a) domestic regulatory requirements and (b) adoption of non-arbitrary and proportionate contrary measures that seek to achieve a legitimate public interest objective. Article 14.13, concerning the location of computing facilities, mandates that no party shall require the location or use of computing facilities within its territory as a condition to doing business in that territory. The derogations provided under this provision are similar to those under Article 14.11. The provisions in the CPTPP have subsequently been replicated in agreements such as the Digital Economy Partnership Agreement (DEPA).

The RCEP, while broadly similar to the CPTPP and DEPA, provides a somewhat greater latitude to parties in regulating cross-border data flows by specifically recognising that parties may adopt measures to restrict cross-border data flows to protect their essential security interests. These measures cannot be questioned whatsoever. In addition, the RCEP lacks a specific enforcement mechanism, implying that its provisions are more voluntary in nature.

The most restrictive provisions pertaining to cross-border data flows are found in the USMCA, which is widely regarded as one of the most "pro Big-Tech" free trade agreements.[8] Article 19.11 of the USMCA provides that: "No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person." This provision is subject to exceptions that permit the implementation of domestic regulatory measures (to restrict cross-border flows of data) that are "necessary to achieve a legitimate public policy objective" and that are not (a) applied in a manner so as to constitute an arbitrary or unjustifiable discrimination or a disguised restriction on trade and (b) do not impose restrictions on transfer of data greater than necessary to achieve the relevant public policy objective. Further, Article 19.12 of the USMCA restricts signatories from requiring computing facilities to be located domestically as a condition to conduct business in that territory.[9]

These provisions significantly limit a country's ability to implement measures that seek to protect personal data privacy. The provisions are not only mandatory in nature, but they also contain very limited exceptions that can make it difficult to justify the use of any contrary domestic measures.[10] Notably, the USMCA goes further than the CPTPP in restricting domestic regulation of cross-border data flows by: (a) barring the adoption of measures that restrict cross-border data flows (as opposed to requiring parties to permit cross border data flows), (b) removing the recognition that parties may have their own regulatory requirements, and (c) imposing a "necessity" requirement for domestic measures that restrict cross-border data flows.

In this context, it is worth noting that the EU has been wary of the inclusion of USMCA-style free flow of data clauses in the JSI, fearing that its domestic regulatory regime, which sets a high standard of data protection, may come under threat.[11] The EU has instead sought to include provisions that specifically recognize the ability of countries to implement restrictions on cross-border transfers on grounds of protecting privacy.[12] The United States has also recently withdrawn its support for proposals concerning strict rules at the WTO's JSI that would liberalize cross-border data flows, seemingly to re-evaluate how technology companies should be regulated in the public and consumer interest.[13]

Overall, each of the agreements referred to above restricts the ability of countries to regulate the data economy in the interests of consumers and the general public. Thus, the issue of whether and how to regulate cross-border data flows is one of the more critical and contentious issues on the agenda in a number of trade agreements currently under negotiation. This includes regional agreements such as the Indo-Pacific Economic Framework for Prosperity (IPEF) as well as bilateral agreements such as the U.S.-Kenya Strategic Trade and Investment Partnership (STIP).

CONCLUSIONS

Provisions that restrict the regulation of cross-border data flows can limit the ability of States to implement domestic measures to protect the privacy and security of consumer data.

By enabling the unrestricted flow of data to jurisdictions with low standards of privacy protection, consumer interests are harmed. Companies can escape accountability for how they use and commercialize personal data. By enabling data to be transferred to countries with low standards of privacy and data protection, free trade agreements privilege corporate economic interests over core values of privacy and human rights. From a consumer and digital rights perspective, the logic should be the opposite: the protection of people's rights should come first.

Rather than seeking to adopt binding measures that force countries to enable unrestricted cross-border flows of data, international trade agreements should either avoid such provisions altogether or adopt less restrictive approaches. This could be done, for instance, by using voluntary instead of mandatory language or by carving out specific and unqualified prudential exceptions providing for restrictions on cross-border data transfers to protect consumer privacy. Such an approach could secure a privacy friendly outcome, thereby improving consumer trust in the global digital economy. It would also create new business incentives and enable innovation for privacy-friendly, human-centric technology.

FURTHER READING:

- Kristina Irion et al., Trade and Privacy: Complicated Bedfellows, University of Amsterdam, July 2016, https://www.beuc.eu/sites/default/files/publications/beuc-x-2016-070_trade_and_privacy-complicated_bedfellows_study.pdf
- Privacy International, Privacy is not a commodity to be traded, https://privacyinternational.org/news-analysis/1407/privacy-not-commodity-be-traded
- Privacy International, Our Data is not For Trade, https://privacyinternational.org/taxonomy/term/678
- Rishab Bailey and Smriti Parsheera, "Data Localisation in India: Questioning the Means and Ends", NIPFP Working Paper No 242, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3356617
- Anita Gurumurthy et al., The Grand Myth Of Cross-Border Data Flows In Trade Deals, IT For Change, 2017, http://itforchange.net/grand-myth-of-cross-border-data-flows-trade-deals#footnote34_7w9cffs

ENDNOTES:

[1] Francesca Casalini et al., *Cross-border data flows: Taking stock of key policies and initiatives*, OECD, October 2022, https://read.oecd-ilibrary.org/science-and-technology/cross-border-data-flows_5031dd97-en#page4

[2] *Id.*

[3] Rishab Bailey and Smriti Parsheera, "Data Localisation in India: Questioning the Means and Ends", NIPFP Working Paper No 242, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3356617

[4] Digital Trade Alliance et al., *Consumer and Digital Rights Groups Call on the International Joint Initiative on E-Commerce to Safeguard Data Protection and Privacy*, https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-112_-_global_statement_to_safeguard_data_protection_and_privacy_in_the_wto_joint_statement_initiative_on_e-commerce.pdf

[5] Consumers International and VZBV, *Indicators of Consumer Protection and Empowerment in the Digital World*, 2017, https://www.vzbv.de/sites/default/files/downloads/2017/03/13/conpol_stats_breakdown.pdf; CIGI-IPSOS, *Global Survey on Internet Security and Trust*, 2019, https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/

[6] A transfer to a foreign jurisdiction may be conducted pursuant to a finding by the European Commission that the foreign country adequately protects the data or pursuant to appropriate safeguards being adopted such as the implementation of binding corporate rules. The GDPR also provides for certain limited exceptions to the above, such as where explicit consent of the data subject has been secured, the transfer is necessary to conclude a contract between the parties, or where the transfer is necessary for public interest reasons.

[7] Yasmin Ismail, "E Commerce Joint Statement Initiative Negotiations Among WTO Members: State of Play and Impact of Covid-19", International Institute for Sustainable Development and CUTS International, April 2021, https://www.iisd.org/system/files/2021-04/e-commerce-negotiations-wto-members-covid-19.pdf

[8] Daniel Rangel and Lori Wallach, *International Pre-emption by "Trade" Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Practices, Rethink Trade*, March 2023, https://rethinktrade.org/wp-content/uploads/2023/03/International-Preemption-by-Trade-Agreement.pdf; Jeanne Whalen, *Trump's USMCA delivers big wins to drugmakers, oil companies and tech firms*, The Washington Post, October 2, 2018, https://www.washingtonpost.com/business/economy/trumps-usmca-delivers-big-wins-to-drugmakers-oil-companies-and-tech-firms/2018/10/02/2d68ad10-c66f-11e8-b1ed-1d2d65b86d0c_story.html

[9] Separately, Article 17.18 of the USMCA allows restrictions on cross-border data flows to be implemented regarding financial payments in certain circumstances where sectoral regulators are not provided immediate, ongoing, and direct access to financial data required for their regulatory and supervisory roles and such failure is not remedied.

[10] Any contrary measure must meet tests of necessity, proportionality, and non-arbitrariness. These are said to be extremely high standards, making it difficult for any contrary measure to be implemented. Michael Geist, *Data Rules in Modern Trade Agreements: Towards Reconciling an Open Internet with Privacy and Security Safeguards,* in CIGI (ed), Special Report: Data Governance in the Digital Age, Waterloo, CIGI, 2018, *cf.* Patrick Leblond, *Uploading CPTPP and USMCA Provisions to the WTO's Digital Trade Negotiations Poses Challenges for National Data Regulation,* in Mira Burri (Ed), Big Data and Global Trade Law, Cambridge University Press, July 2021, https://www.cambridge.org/core/books/big-data-and-global-trade-law/uploading-cptpp-and-usmca-provisions-to-the-wtos-digital-trade-negotiations-poses-challenges-for-national-data-regulation/59483E5412CA936C31F6EBCF9CD97FDF

[11] Yasmin Ismail, *E-Commerce Joint Statement Initiative Negotiations among World Trade Organisation Members: State of Play and the Impact of COVID-19,* IISD and CUTS International, 2021, https://www.iisd.org/system/files/2021-04/e-commerce-negotiations-wto-members-covid-19.pdf; European Parliament, *At a Glance: WTO Ecommerce Negotiations,* 2020, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf

[12] *Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments relating to Electronic Commerce*, World Trade Organisation, April 26, 2019, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.