

Trade, Privacy and Cross-Border Data Flows

Today international trade (goods, services and digital) is dependent on an exchange of information that is enabled by open, cross border data flows (CBDF). This note briefly explores how ‘cyber diplomacy’; the intersection of issues of human rights, security and economic policy, may be the catalyst for continued growth to facilitate digital trade, improve productivity and contribute to people’s wellbeing.

Digital trade layers on top of E – Commerce and may be defined to include the use of the Internet to manufacture, create, search, purchase, sell, and deliver a good or service, (including information), across borders, together with open market access to the flow of information/data on non-discriminatory grounds.

Digital trade is estimated to account for 25 percent of global GDP today and as much as 50 percent of value creation going forward, according to the Global Trade and Innovation Policy Alliance (GTIPA), an alliance of 43 think tanks.¹

International digital trade is dependent on a free flow of commercial information across borders and permissioned access to that information by legitimate parties, no matter where the data is stored or processed. Regulatory pressures have been steadily rising in many parts of the world which have affected CBDF. This has led to some countries proposing or implementing data protection laws in a way that restricts CBDF’s disproportionately, usually citing concerns regarding their citizen’s personal privacy or national security.

Data protection and CBDF is now core to a modern economy; the movement of data is as important as the movement of goods and other trade in services to stimulate growth and innovation at home and to facilitate cross border trade. The more individual countries regard each other as having an adequate level of protection, the greater the economic area within which data can circulate freely and yield measurable benefits.

The OECD has supported privacy as a fundamental value and a condition for the free flow of personal data across borders since 1980². The EU General Data Protection Regulation (GDPR)³ firmly asserts control of this data belongs to the citizen; a complimentary initiative is the Council of Europe (COE) Convention 108⁴ also recognises the importance of CBDF.

Therefore ensuring data flows freely commences with individual countries providing a range of mechanisms for ordinary businesses of all sizes to be able to legitimately communicate and use data dependent services wherever they chose to do business.

Data protection (DP) has always been about both protecting privacy and human rights and ensuring the free circulation of data, including across borders. The UN recognised the right to privacy in the digital age in 2016⁵.

To reflect the importance of CBDF’s the UN in 2016 amended Article 19 of the Universal Declaration of Human Rights (UDHR)⁶ that it considers the internet to be a human right as it permits the free flow of information.

¹ <https://gtipa.org/organizations>

² <https://www.oecd.org/sti/ieconomy/privacy.htm>

³ <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

⁴ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>

⁵ https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

Sadly this is not a universal view. In the US, the USTR reports annually on CBDF⁷. The Information Technology and Innovation Foundation has mapped countries where CBDF is restricted. In a July 2021 report they said that 62 countries have imposed 144 data-localization measures, while 38 other restrictions have been proposed or are under consideration⁸.

There is a clear relationship between the concept of 'cyber diplomacy'; the intersection of issues of human rights, security and economic policy underpinning responsible international trade, and trade agreements. The treatment of data flows in privacy regulations contained in multilateral, plurilateral and bilateral trade agreements such as the WTO, AfCFTA, RCEP, CPTPP, DEPA etc, (plus the OECD, G20) and their protocols and schedules, increasingly have a digital component or in the case of the DEPA, are exclusively focused on digital trade.

Let's look at the major multilateral and regional trade agreements in order of signing.

WTO: The Geneva Ministerial Declaration on Global Electronic Commerce, 1998.

AfCFTA: The African Continental Free Trade Area is a multilateral trade and economic agreement between 45 African Union member states that was agreed in 2015. Protocols on E- Commerce are now being negotiated.

ASEAN: The 10 members of ASEAN signed the ASEAN Agreement on E-Commerce in November 2018. The Agreement includes provisions on CBDF, which may become binding by 2025.

CPTPP: The Comprehensive and Progressive Trans-Pacific Partnership, (CPTPP) is an 11 country trade bloc in the Pacific Rim that was agreed in 2018. The Agreement includes binding provisions on CBDF.

AfCFTA - The African Continental Free Trade Area, a 44 country was signed in 2018, with a Digital Trade Protocol (AfCFTA DTP) added in 2024. The Agreement includes provisions on CBDF, which may become binding.

U.S. - Japan: The US-Japan Digital Trade Agreement, a bilateral trade agreement entered into force in October 2019. The Agreement includes binding provisions on CBDF.

RCEP: The Regional Comprehensive Economic Partnership (RCEP) is a 15 member economic bloc in East Asia-Pacific that was signed in 2020. The Agreement includes provisions on CBDF.

DEPA: Digital Economy Partnership Agreement, a plurilateral trade agreement between Singapore, New Zealand and Chile, entered into force in June 2020. The Agreement includes binding provisions on CBDF.

SADEA - The Singapore – Australia Digital Economy Agreement, a bilateral trade agreement focussing on digital trade entered into force in December 2020. The Agreement includes binding provisions on CBDF.

Some of the above agreements still have to be ratified e.g. the RCEP and CPTPP. In addition to the above binding trade agreements, other multilateral organisations also influence digital trade.

The World Bank, OECD, and G20: Have proposed a global Digital Data Tax and a Global Internet Tax Agency to provide legal certainty on cross border digital tax issues. The G20 Issued the 'Osaka

⁶ https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

⁷ <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>

⁸ <https://itif.org/sites/default/files/2021-data-localization.pdf>

Declaration on the Digital Economy’ at the G20 Osaka Summit, 2019. The UN through UNCTAD has further weighed in with a 2021 report on what is at stake for developing economies in the WTO negotiations on E-Commerce.

The WTO is the preeminent rule setting and negotiating forum for global trade. It is the ultimate arbiter of inter country trade disputes and its rules are binding. With respect to the wider concept of digital trade, the Geneva Ministerial Declaration on Global Electronic Commerce in 1998 gave the impetus for a more inclusive trade agreement for international digital trade⁹.

In January 2019, 78 members of the WTO, confirmed intentions to launch negotiations on trade related aspects of E-Commerce as the ‘WTO Joint Statement Initiative (JSI) on E-Commerce’ with the current participation of 86 members¹⁰. The JSI will accelerate the negotiations aiming to deliver substantial progress by the 12th WTO Ministerial Conference (MC12) which has been rescheduled to 30 November to 3 December 2021¹¹.

The pandemic has given a huge jolt to those that are still hesitant about enabling data flows. Embracing the digital world was forced upon the entire world by the COVID -19 pandemic in a matter of months.

In retail banking for example, large banks reported ATM use declined by up to a third, while online transactions increased by a similar amount or even more in some countries.¹² In global commerce, without a free flow of information the adverse economic effects of the pandemic would have been multiplied. Cyber diplomacy is here to stay and grow.

In a subsequent paper I will explore how this may be negotiated and integrated as part of binding trade agreements.

About the writer. Mr [Michael Mudd](#) is a digital trade economist and Senior Digital Trade Adviser to International Economics Consulting Ltd. He specialises in analysis and advisory, providing opinion and insight into policy, knowledge management, data security and digital transformation for trade in Asia-Pacific, Africa and the Middle East.

He is an appointed IT standards expert to JTC-1 of the ISO. He is a member of the policy committee of the Hong Kong Computer Society and a member of the Government of Hong Kong’s Expert Group on Cloud Computing. He is the Chairman of the Public Policy Working Group of the Middle East & North Africa Cloud Alliance (MENACA).

He may be contacted at asiapolicypartners@outlook.com

⁹ https://www.wto.org/english/tratop_e/ecom_e/mindecl_e.htm

¹⁰ <https://www.mfat.govt.nz/assets/Trade-agreements/WTO-e-commerce-negotiations/WORK-PROGRAMME-ON-ELECTRONIC-COMMERCE-Ministerial-Decision-December-2017.pdf>

¹¹ https://www.wto.org/english/thewto_e/minist_e/mc12_e/mc12_e.htm

¹² <https://www.theguardian.com/australia-news/2020/jun/03/fewer-atms-no-more-cheques-and-lower-e-payment-fees-predicted-for-australia-in-wake-of-coronavirus>