CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Global Rules of Digital Trade: Can We Adapt Bordered Regulation for a Borderless World?

by Laura Dawson

February 2018

INTERNATIONAL TRADE SERIES

GLOBAL RULES OF DIGITAL TRADE: CAN WE ADAPT BORDERED REGULATION FOR A BORDERLESS WORLD?

by Laura Dawson

CGAI Advisory Council Member
February 2018

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 421 – 7th Avenue S.W., Calgary, AB T2P 4K9
www.cgai.ca

ISBN: 978-1-988493-96-1

How big is the gap between where we are and where we need to be?

The rules of global trade originated for farm products and manufactured goods – things that can drop on your foot. The addition of rules governing non-physical tradables in the 1990s, such as services and intellectual property (IP), challenged the goods regime. We are increasingly trying to stretch the rules meant to govern the sale of a bushel of corn to govern the transmission of electronic signals representing billions of bytes of data. Trade rules for goods are built on the premise that we are able to identify the geographic origin of the product and attach a tariff or other condition on its international sale, usually at the point where the product crosses the border. Digital products by contrast are not bound by geography, nationality or even physical properties. Thus, rule making for this new kind of trade will be very difficult indeed.

Intellectual property rules are mostly about protecting ownership of ideas, processes and technologies, and thwarting attempts by non-owners to use IP without paying for it or in ways that would diminish its value. In the case of handbags and cellphones, IP enforcement can take place at the border if customs officials are able to distinguish fakes from the genuine article, but digital products present enormous challenges to those who try to police the trade in ill-gotten movies, software and digital designs, since transactions move directly between buyer and seller – directly, invisibly and in enormous volumes.

Cross-border services are also difficult to monitor, and thus harder to regulate, but conventional services trade most often involves the movement of a person – either the provider or a consumer – across a physical border. This meant that most services transactions were subject to some form of border monitoring. Widespread, systemic abuse was unlikely because a single person could not deliver or consume thousands of extra-legal services transactions in a single day. Fast-forward to the world of digital trade and it is entirely possible for a digital service provider to conduct tens of thousands of transactions in a single minute.

Perhaps we don't need trade rules for the digital economy. How much of the original rationale for trade rules is applicable to the digital economy? The general purpose of goods trade rules is to protect consumer safety and protect producers from having their products or IP stolen, together with ancillary public policy motivations such as creating cost barriers to protect domestic manufacturers from lower cost imports. Trade rules also provide a means of tracking goods crossing the border so that governments can collect taxes on the product's sale.

When applied to digital trade, these original objectives – with a few modifications – remain relevant. They include:

1. Protection of consumers from fraud and misuse of personal information;
2. Protection of legitimate public policy goals, such as a government's right to access information in other locales (or in the cloud) for law enforcement or national security purposes;

3. Protection of intellectual property rights; and

4. Promotion of the development of digital enterprises.

The last objective is perhaps the most challenging because it involves a range of incentives, such as R&D tax credits, that may or may not be effective. Also, some of the other objectives designed to protect consumers may tie the hands of digital enterprises to such an extent that investment and employment move elsewhere. In an era where policy lags behind rapidly changing technology, governments walk a fine line between providing the constraints necessary to protect individual and corporate rights while also providing the freedoms and incentives to develop robust and competitive digital enterprises.

The stakes are high. McKinsey Global Institute reports that cross-border data flows in 2015 were 45 times larger than they were a decade earlier. By 2020, they are forecast to grow another nine times. Within this same period, cross-border movement of goods and investment has flattened or declined. This has a direct impact at home. Meanwhile, digital trade is robust and growing. U.S. government sources estimate that digitally enabled services account for 52 per cent of all U.S. services to Canada and 46 per cent of all services imports from Canada.

Figure 1: *Opponents of Airbnb rally before a regulation hearing in New York City. (Shannon Stapleton/Reuters)*

The regulatory challenges are enormous. Technology is moving faster than regulation. Today's problems might be moot by the time we have an effective regulatory regime to deal with them and the challenges of tomorrow have not even occurred to today's regulators. The gap between

applied technology and regulation, known as regulatory arbitrage, is being successfully exploited by developers of new service delivery platforms such as Uber and Airbnb. These enterprises disrupt traditional, regulated services by providing new mechanisms of direct service delivery. In doing so, disruptors make a bet that they can operate for a period of time while government policy lags, before being subject to updated rules that might put them out of business.

A second problem stems from the fact that if you can't measure it, you can't regulate it. Rapid technological changes mean that we don't have an accurate understanding of the true dimensions of digital services trade. Trade transactions are quantified and taxed when a product crosses the border. Without a customs declaration, no trade has taken place except what sellers self-report for tax purposes. As organizations such as the OECD note, government enforcement authorities remain in the dark when neither the buyer nor the seller reports a digital service transaction to a government.

Add to this the volume of trade that is possible when geography, shipping and other constraints of the physical world are no longer an issue and it is clear that there is a huge and growing part of the global economy that we know very little about.

Finally, there is a problem of fragmentation. There is no one global digital services organization charged with regulating cross-border digital trade. Trade agreements are picking up the slack, but the regulatory regimes that are emerging from these different institutional venues are fragmented and their effectiveness and enforceability are very much an open question.

None of this bodes well for the near future of digital trade rule-making and a weak understanding of the scope, nature and economic importance of digital trade makes it difficult to decide how to direct and shape trade, investment, and business and workforce development policies.

Technology turns trade on its head

New technologies give rise to new ways to create and deliver goods and services and these technologies are upending the way we think about trade rules. A few examples below help to illustrate the emerging challenges.

3D Printing

With additive or 3D printing, a designer in Country A provides a template for a 3D-printable item to a customer in Country B. The file is downloaded from the cloud while the financial transaction is completed somewhere in the world, not necessarily related to where either the designer or the customer resides. The customer completes the transaction by creating the product on his or her 3D printer, but no physical product has crossed the border so no collection of customs tariffs or other border taxes is possible. Similarly, there is no use of conventional trade instruments such as rules of origin, quotas, export controls or duty drawbacks. So what

was traded? A good? A service? What is taxable? What if the product breaks, causing harm to someone? Who is liable?

Digitally Enabled Goods

Digitally enabled goods refer to products where a growing share of a product's function and value is provided by smart technologies. Today, the two-century old John Deere company is fast becoming a technology company that delivers agricultural automation tools via tractor. When customers buy a tractor from Deere, they also get access to the platform MyJohnDeere, a big data analytics tool that helps producers optimize the management of production data, equipment information and farm operations.

Figure 2: *A farmer using the MyJohnDeere app in an effort to optimize the management of his crops. (MachineFinder Blog)*

Digitally enabled goods pose a particular challenge for trade regulators. Once a conventional goods transaction is completed, it falls off the regulatory radar screen, but digitally enabled goods bring with them continuing questions of IP ownership, movement of data and the value of continuing services trade.

Blockchain

Blockchain is a distributed network that functions as a giant global spreadsheet shared across millions of computers worldwide. The network is a continuously growing database with

safeguards against tampering and fraud. Blockchain can be used by manufacturers to maintain accurate inventory and shipping records with their input suppliers, or it can be used to facilitate cross-border payments. In the pre-digital age, verification of payments in cross-border trade was a time-consuming and risky enterprise. Blockchain technology cuts risk precipitously and makes payments practically instantaneous. The shipping giant Maersk now uses blockchain technology instead of paper-based bills of lading.

While the reliability of blockchain technology is still evolving, its use is growing by leaps and bounds. But, having ledgers in the cloud that are simultaneously everywhere and nowhere is a huge challenge for makers of trade rules who have for centuries relied on the geographic location of transactions and the national origin of products as a basis for decision-making.

Where does public interest intersect with digital trade?

Digital trade rules are developing along three key tracks:

- protect people's privacy
- protect intellectual property
- create an enabling environment for innovation

Protect Privacy

The collection and management of personal information is one of the most contentious areas of digital trade. While the intention is to ensure that people's personal data are not misused or mishandled, many national regulators have defaulted to requiring that their citizens' data be contained within national borders. This practice, called data localization, focuses more on geography as a guarantee of safety rather than on establishing enforceable, generalized standards for data management.

The Canadian provinces of British Columbia and Nova Scotia join China, Russia and Vietnam in demanding that companies store data on servers physically located within their borders. Other jurisdictions allow some information to flow freely but block the movement of accounting, tax, financial and personnel information from moving across electronic borders.

By insisting that data be stored on domestic servers and tended by domestic managers, governments create extra costs for firms whose profitability depends on the scale benefits provided by cloud computing and globally aggregated services. A 2015 study by Leviathan Security Group estimates that data localization drives up computing costs by 40 to 60 per cent.

One of the ironies of data localization is that it actually might make consumers less secure. On Nov. 18, 2017, the U.S. Chamber of Commerce opposed the Brazilian Central Bank's proposed cyber-security regulations that would bar financial institutions such as Citibank and JPMorgan

Chase from using data processing and cloud computing services based abroad. The Chamber claimed that not only would such a prohibition raise costs, it would make fraud detection more difficult.

Protect Intellectual Property

The new digital IP issues resemble the concerns of pre-digital IP rights but the nature of the technology provides a new spin on old problems. One of these new concerns is the issue of intermediary liability where online service providers and intermediaries such as Google and YouTube are asking that they not be held liable for copyright violations on material they host or that is uploaded by their users. The intermediaries' position is that they should not be held responsible for third-party content. Moreover, relegating them to the role of enforcer makes the internet "less free, innovative, and collaborative." A June 2017 press release from the Internet Association claims that nearly 80 per cent of venture capital investors are less likely to invest in services where protections from intermediary liability do not exist. Another problem is the demand by governments for foreign entities to reveal source code and other IP in order to protect national security or encourage domestic economic development. The Software Alliance responds that demands for source code "pose significant inherent risk to intellectual property" while providing little security value.

Similarly, there have been a number of recent high-profile cases where companies have been asked to unlock the IT devices of individuals involved in criminal investigations, such as the Apple iPhone owned by the 2017 Texas church shooter.

Enable Innovation and Support Digital Business

As discussed above, too much emphasis on privacy protection through localization or zealous enforcement of intellectual property rights may hamper the ability to create new products and processes or to fully maximize the benefits of the digital economy.

A contentious issue for Canada is the de minimis threshold that exempts low-value shipments from border taxes and duties. In Canada, that level is $20. E-commerce enterprises in the United States – where the de minimis level is $800 – argue that the low Canadian levels hinder the growth of cross-border e-commerce. Moreover, the costs of administering low-value shipments outweigh the benefits in taxes. A C.D. Howe study suggests that the federal government would save $161 million per year by raising the de minimis rate. The Retail Council of Canada counters that Canadian retailers could not compete against the tax-free advantage that e-commerce purchases from the U.S. would enjoy since there is not currently any mechanism for federal or provincial sales tax collection on cross-border purchases.

Where is the new generation of digital trade rules coming from?

TPP and NAFTA

The 1994 North American Free Trade Agreement (NAFTA) contains few provisions that are directly relevant to digital trade. (Most people did not have internet in their homes when the agreement was negotiated.) But, the basic principles of transparency, non-discrimination, protection of intellectual property and avoiding rules that can be used as disguised barriers to trade, provide a good framework upon which to build a new digital regime.

The Trans-Pacific Partnership (TPP) represents a concerted effort, led by the United States, to establish a number of key digital trade principles in legal text. The Digital 2 Dozen, published on the website of the office of the United States Trade Representative, provides a list of U.S. priorities for a new digital trade regime, led by principles of freedom, openness and non-discrimination.

Since the U.S. withdrew from the TPP, leaving the other 11 negotiating parties to sign a similar, but not identical, replacement agreement, the U.S. is facing a gap in its attempts to lead the charge on digital trade rules. An opportunity exists to continue this leadership in a more limited form by installing the TPP rules in NAFTA, currently under renegotiation. This should not be too difficult since the three NAFTA parties were all original TPP signatories and had previously agreed to the TPP digital provisions. However, as politics, interests and technologies change, there is no guarantee that this will be a smooth transition.

Intermediate Liability

The NAFTA negotiations are still in an early stage, but officials report that talks on the digital chapter are going well with the exception of intermediate liability. The U.S., perhaps influenced by its powerful domestic entertainment lobby, is pushing for strengthened liability provisions. Canada is pushing back against expanded liability and this position is shared by many powerful U.S. entities such as the Internet Association, which argues that its members are already supporting the protection of intellectual property and public decency through other regulatory measures.

Government Procurement

In the NAFTA government procurement negotiations, U.S. firms are calling for greater openness in Canadian federal and provincial government services that require Canadian user data to be housed on servers located in Canada. At the same time, the U.S. is proposing severely curtailing the access that Mexico and Canada currently enjoy in many U.S. government sectors – a predictable position for an administration elected on a Buy American, Hire American platform. Given the rancour in this sector overall, it is unlikely that Canada will yield much new access in digital government services, even if the U.S. can guarantee safe handling of Canadian data.

The Special Case of Financial Services

Another element of uncertainty in the interplay between TPP and NAFTA is the issue of data localization for financial services companies. In the original TPP, signatories agreed to prohibit data localization (i.e., to insist on free flow of digital data across borders) for all sectors *except* financial services. This exclusion was meant to reflect the special status of financial services

Regulating the international movement of financial services hinges on the balance between business demands to eliminate trade barriers and regulators' requirements to have access to the information they need.

The 2008-2009 financial crisis emphasized to U.S. financial regulators the need to have secure and timely access to financial data. The U.S. Treasury Department and key U.S. financial institutions formed an influential bloc seeking to keep financial services out of the broader data liberalization measures in the TPP, staking out a distinct position against their own country's trade negotiators.

Once the negotiations were completed, however, it became clear that the U.S. Congress was unlikely to authorize the TPP with a data exemption for financial services. Thus, in early 2016, then-Treasury secretary Jack Lew proposed a set of compromise positions, chief among them that the financial services sector would not use data localization as long as regulators were able to access information stored abroad.

Since the U.S. withdrew from the TPP in January 2017, the Lew proposal was never tested but the Lew principles provide a guide to U.S. preferences in future negotiations such as NAFTA, the Trade in Services Agreement (TiSA) and the U.S.-EU Transatlantic Trade and Investment Partnership (TTIP).

Data Protection and the EU

The European Union has been at the forefront of the development of data protection rules. Unlike the TPP, which prohibits interruptions to cross-border data flow except in limited circumstances, the EU only permits cross-border data flow when the other territory can prove that it is capable of providing an adequate level of protection. Such proof relies on the implementation of EU-sanctioned privacy frameworks regulating the collection, use and disclosure of personal information.

As a partner in this recognition and verification process, Canada implemented the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 2001. EU member states operate within a similar framework, the General Data Protection Rule (GDPR). Third-party countries are prevented from transfers of personal information from the EU unless they implement similar safeguard measures. The U.S. and EU implemented a more up-to-date privacy shield framework in 2016, but despite temporary peace between these two economic giants, the global rules are far from set. At present, the EU is the global standard bearer for

consumers' rights to privacy, setting itself as an obstacle to companies who want to access users' personal data to better market their services or others with more nefarious intent.

WTO

The World Trade Organization rules provide the template upon which other trade agreement texts are created, so it makes sense that the WTO should be a focal point for the emerging area of digital trade governance. Also helpful are principles to ensure that trade rules not be used as a disguised barrier to trade and approaches to trade facilitation at the border which can be adapted from traditional trade to e-commerce.

Many companies, including China's Huawei, argue in favour of using the multilateral WTO system as the arbiter of digital trade rules and dispute settlement, rather than allowing the emerging rules regime to devolve into fragmented arrangements through regional agreements such as the TPP.

Negotiations are ongoing within the WTO for a new TiSA. However, participation in the agreement is voluntary and includes only a small percentage of the WTO's 164 members. Within the TiSA, the U.S. is attempting to extend its global ban on data localization.

China

The differences between the United States and the European Union regarding cross-border information flows are more a matter of degree than of principle, compared to the closed, national system that exists within China's "great firewall". China's 2017 cyber-security law requires that data must be stored inside the People's Republic and subject to various national data retention regulations and that digital equipment be subject to mandatory security inspections.

China's closed cyber-regime has led to the lopsided dynamic of foreign firms selling their stake in Chinese firms while Chinese firms leverage their market power and technology to expand into the West. In November 2017, Amazon Web Services sold its cloud computing servers in China to Beijing Sinnet Technology to comply with China's data localization requirements.

At the same time, while the Chinese market is a huge national market, Chinese service providers and AI companies may find that localization rules prevent them from developing the kind of new technologies and new efficiencies that can be generated from a fully global scale. For example, one of the new regulations requires all health and medical data on Chinese citizens to be stored on servers located inside the People's Republic. IBM has an application designed to compare health records of Chinese citizens against a global disease database but because a Chinese hospital is prohibited from sending patient data outside the country, its records can only be compared against the smaller Chinese sample. Without access to big data, Chinese analysis will be based on medium-sized data with potentially less robust outcomes.

Where do we go from here?

From a regulatory perspective, China's restrictive digital policies put it at the 'mostly closed' end of the spectrum while the United States and even the European Union can be described as 'mostly open'. As global rules develop, we can expect that these three large markets and their regulatory preferences will fundamentally shape the digital trade rules regimes affecting smaller countries like Canada. But even for those countries whose regulatory impulses lean toward an open internet and support for digital business, their liberalizing intent will be tempered by demands to provide stricter protections for intellectual property rights and for consumer privacy.

The WTO, meanwhile, provides a strong framework for progress, albeit very slowly. The glacial pace of trade negotiations compared to the rapid pace of technological change ensures that regulatory gaps will continue. While some enterprises can profit from temporary rules gaps, the absence of transparent, enforceable digital rules of the road will prevent other firms from achieving global reach and scale.

Closer to home, the digital modernization chapter of a prospective NAFTA 2.0 agreement is not likely to yield much beyond what was agreed to in the TPP because the political frictions affecting the current negotiations will get in the way of fulfilling a more ambitious digital modernization agenda, despite strong consensus among all three countries for building North America's digital competitiveness in the world.

About the Author

ABOUT THE AUTHOR

Laura Dawson is Director of the Canada Institute at the Wilson Center in Washington D.C. Named one of Canada's Top 100 foreign policy influencers by the Hill Times in 2014, Dawson is a speaker, writer, and thought leader on Canada-U.S., NAFTA, TPP, and international trade issues. Previously, she served as senior advisor on economic affairs at the United States Embassy in Ottawa and taught international trade and Canada-U.S. relations at the Norman Paterson School of International Affairs. Dawson continues to serve as Emeritus Advisor at Dawson Strategic, which provides advice to business on cross-border trade, market access and regulatory issues. She is an Advisory Council member of the Canadian Global Affairs Institute and serves on the board of the Council of the Great Lakes Region. Dawson holds a PhD in political science.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.