CEPR PRESS

Edited by Ingo Borchert and L. Alan Winters

Addressing Impediments to Digital Trade

UKTPO
UK TRADE POLICY OBSERVATORY

UNIVERSITY OF SUSSEX

Addressing Impediments to Digital Trade

CEPR PRESS

Centre for Economic Policy Research
33 Great Sutton Street
London, EC1V 0DX
UK
Tel: +44 (0)20 7183 8801
Email: cepr@cepr.org
Web: www.cepr.org

ISBN: 978-1-912179-42-8

Adressing Impediments to Digital Trade

Edited by Ingo Borchert
and L Alan Winters

CEPR PRESS

CENTRE FOR ECONOMIC POLICY RESEARCH (CEPR)

The Centre for Economic Policy Research (CEPR) is a network of over 1,500 research economists based mostly in European universities. The Centre's goal is twofold: to promote world-class research, and to get the policy-relevant results into the hands of key decision-makers.

CEPR's guiding principle is 'Research excellence with policy relevance'.

A registered charity since it was founded in 1983, CEPR is independent of all public and private interest groups. It takes no institutional stand on economic policy matters and its core funding comes from its Institutional Members and sales of publications. Because it draws on such a large network of researchers, its output reflects a broad spectrum of individual viewpoints as well as perspectives drawn from civil society.

CEPR research may include views on policy, but the Trustees of the Centre do not give prior review to its publications. The opinions expressed in this report are those of the authors and not those of CEPR.

UK TRADE POLICY OBSERVATORY (UKTPO)

The UK Trade Policy Observatory, a partnership between the University of Sussex and the Royal Institute for International Affairs (commonly referred to as "Chatham House"), is an interdisciplinary independent expert group of researchers at the University of Sussex covering all aspects of trade.

The UKPTO aims to bring objective and impartial analysis to trade policy debates and policymaking processes by:

i. conducting independent original research on UK and global trade and trade policy;
ii. providing impartial, evidence-based policy advice to stakeholders and policy makers;
iii. providing influential commentary and new contributions to current debates;
iv. offering training on trade and trade policy.

The University of Sussex has the largest collection of academic expertise on the world trading system in the UK, with specialists on trade policy, trade law, trade politics and European law and economy. The team includes experts in economics, international relations, business and management and law.

The Observatory is committed to engaging with a wide variety of stakeholders to ensure that the UK's international trading environment is developed in a manner that benefits all – in Britain and beyond. Further details about the UKTPO and its publications are available online: https://blogs.sussex.ac.uk/uktpo/

Contents

Ministerial preface 1
The Rt Hon John Whittingdale OBE MP

Introduction 3
Ingo Borchert and L. Alan Winters

1 Mapping policies affecting digital trade 19
Simon J. Evenett and Johannes Fritz

2 Mapping approaches to cross-border data flows 45
Javier López-González, Francesca Casalini and Taku Nemoto

3 An AI policy for the (near) future 73
Bryan Mercurio and Ron Yu

4 Source code disclosure: A primer for trade negotiators 105
Cosmina Dorobantu, Florian Ostmann and Christina Hitrova

5 The difficult past and troubled future of digital protectionism 141
Susan Ariel Aaronson

6 Governing cross-border data flows beyond trade agreements to support digital trade: Inspiration from international financial standards-setting bodies 169
Patrick Leblond

7 Rights in data, the public interest, and international trade law 195
Teresa Scassa

8 Asia-Pacific digital trade policy innovation 217
Stephanie Honey

Ministerial preface

The UK Department for Digital, Culture, Media & Sport (DCMS) is delighted to have worked with the UK Trade Policy Observatory at the University of Sussex and the Centre for Economic Policy Research to host a Virtual Conference on "Addressing Impediments to Digital Trade".

Digital trade is essential to the UK economy. Experimental estimates indicate that over half of the UK's services exports to the rest of the world in 2019 were digitally delivered. This trade relies on the free flow of data. Around the world, data flows in 2014 were 45 times larger than in 2005. The value of data flows has overtaken the value of global trade in physical goods.

The UK has now successfully negotiated new digital chapters in free trade agreements with Japan and the EU. The UK–EU Trade and Cooperation Agreement goes further on digital provisions than any other EU trade deal, by including provisions such as a permanent ban on data localisation, and a commitment on Open Government Data.

These deals have set a high bar. But digital trade doesn't stand still. Technology is constantly evolving – making trade easier, quicker and cheaper, and making it possible to trade things that couldn't be traded before. Trade agreements have to keep pace with the opportunities and challenges these changes create. They have to guard against new opportunities for protectionism. They have to recognise and remove new forms of trade barriers. And they have to support governments to tackle new problems like fake news and online harms.

We now want our next generation of digital trade agreements to go beyond existing precedent in order to keep pace with technology and meet these challenges head-on.

But negotiating trade deals is only one part of the puzzle. We also want to ensure that businesses and consumers are able to take advantage of the new opportunities these deals create. To do that, we need to keep track of market conditions around the world – tackling barriers wherever we find them – and we need to ensure that our domestic legal and regulatory framework is fully supportive of new technology.

This eBook summarises the discussions held at the conference, helping us to shape our thinking on these issues. Engaging with experts in this space can have a real impact on shaping our trading relationships. By engaging with academia, we hope to build on our existing discussions with industry stakeholders to develop further our thinking on digital trade.

I hope that the conference, and this accompanying eBook, will be the first of many such engagements with academia as we are eager to maintain a long-term dialogue with digital trade thought leaders.

The Rt Hon John Whittingdale OBE MP
Minister of State for Media and Data

Introduction

Ingo Borchert and L. Alan Winters[1]
University of Sussex and UK Trade Policy Observatory;
University of Sussex, UK Trade Policy Observatory and CEPR

Digital technology – digitisation – is changing the world, gradually at first and now, following the Covid-19 pandemic, in a great rush. It is transforming social norms, social structures, politics, the arts, how and where we work, how firms interact with each other, productivity, indeed almost anything you can think of. These transformations are mandating major changes in behaviour and are promoting what were once relatively straightforward trade-offs to the top of our priorities. For example, how does one reconcile privacy with maintaining a large social circle? And what should be the relative weights placed on privacy and the ease of doing business? Few societies, if any, have managed to achieve consensus on these issues and even if they had, the technical complexity of implementing its conclusions would be considerable because digital activity touches on so many separate aspects of policy. Thus, no government has been entirely comfortable with policymaking in this area.

In addition, digitisation has had another consequence. Because data flows more or less costlessly across borders and because data is arguably valuable, we can all potentially become exporters and importers. And more often than not, individuals are engaged in this exchange of data via digital services without payment, in a process that has been dubbed 'third-party funded digital barter' (Snower and Twomey 2020). Since every country has a national regime defining digital rights and responsibilities (even if it is null by default), every digitally active individual essentially becomes a 'multinational' because he or she is dealing simultaneously with multiple jurisdictions. Thus the distinction between national policy and international trade policy has been blurred. As Tim Wu observed (quoted in Aaronson 2019), "almost by accident, the [world trading system] has put itself in an oversight position for most of the national laws and practices that regulate the Internet" (Wu 2006: 263–264). For example, an essentially internal policy, the EU's May 2018 implementation of the General Data Protection Regulation (GDPR) led to changes that required 500 million people to accede to new terms of trade in their data, and companies to change their policies worldwide, affecting a further four billion individuals.

1 The views expressed in this Introduction are those of the authors

A MULTIPOLAR WORLD THAT IS DRIFTING APART

The major Western players in this space – the US and the EU – have very different philosophies towards data and digital activity and are keen to establish their respective approaches as global standards. Thus, digital trade has become the most active frontier of international trade negotiations, with the US proposing rather open rules in its trade agreements and the EU placing a much greater emphasis on privacy in bilateral processes; in fact, the EU approach accords privacy the status and protection of a human right in a horizontal manner that binds both state and private actors across all sectors alike. Due to the EU's economic heft, deep digital intercourse with the Union is for most trade partners tantamount to accepting the EU model. The rivalry over data governance supremacy between the US and the EU leaves out China, which has a quite different approach again and which seems unwilling to compromise it much. Given its size and access to vast troves of local data, China has significant power in this area and if the world is not to fragment further into different digital realms, China will need to be engaged with.

A number of smaller powers in Asia and the Pacific have made far-reaching agreements between themselves, which may point to the way forward by acting as examples for developments elsewhere. But the dilemma for medium-sized economies such as the UK, which need to trade digitally with the major players in order to achieve reasonable scale, is acute. Without a deep national conversation, countries (governments) do not have a well-defined idea of what they require by way of regulation on digital activity; as a result, engaging in binding international negotiations is risky. There is a danger of agreeing to provisions that do not suit local views, which could add further grist to the mill of those opposing trade agreements and, in the extreme, could throw the entire business of making international agreements into disrepute. On the other hand, if countries defined their national structures rigidly in advance, reaching international agreement and easing the world towards a global solution would become very difficult.

WHAT IS AT STAKE WHEN DEALING WITH DIGITAL TRADE

A natural question is to what extent digital activity matters economically as well as socially and politically. Measuring digital trade is formidably challenging (e.g. DCMS 2020), but such trade seems large. The McKinsey Global Institute (2016) finds that "over a decade, all types of flows acting together have raised world GDP by 10.1% over what would have resulted in a world without any cross-border flows. This value amounted to some $7.8 trillion in 2014 alone, and data flows account for $2.8 trillion of this impact." The EU reports that globally, e-commerce sales (one element of digital trade) were estimated at €3.2 trillion in 2019, with around 1.5 billion people shopping online.[2]

2 See https://trade.ec.europa.eu/access-to-markets/en/content/digital-trade-0

In 2019, e-commerce sales by UK businesses were worth £668 billion (ONS 2021). Whilst the majority of these sales arise from within the UK, orders worth £118 billion were received from abroad. These figures demonstrate the significance of digital transactions for UK trade. Moreover, it is well recognised that digital trade offers particular opportunities for SMEs: of the aforementioned e-commerce figures, £4.5 billion worth of overseas sales were captured by UK micro enterprises with fewer than ten employees. The other element of digital trade is digitally delivered services (as opposed to digitally ordered) trade. The sectors in which delivery is potentially electronic, including publishing, software publishing, film and TV, video, radio and music, telecoms, computer programming, consultancy and related activities and information services, accounted for about 7% of UK gross value added in 2019 (DCMS 2021a). Moreover, about £52 billion (or an astounding one-third) of the Digital Sector's gross value added was exported, which underscores the salience of trade openness for the sector's prosperity and, thereby, the UK's growth and employment (DCMS 2021b).[3]

With the size and likely growth of digital trade, the differences in approach to the management of digital activities are leading to increasing concerns about 'digital protectionism'. This concept is poorly defined and poorly understood, since one society's policies to protect privacy, public morals or the integrity of its cyber-infrastructure may look like protectionism from another country's viewpoint. Yet as the above figures demonstrate, the gains from 'getting digital right' are potentially very large. That is why the UK Department for Digital, Culture, Media and Sport and the UK Trade Policy Observatory organised a conference on "Addressing Impediments to Digital Trade", hosted by CEPR, which took place on 1-2 March 2021 and was moderated by Creon Butler of Chatham House. Its aim was to discuss new directions for digital trade policy, including concrete steps to recognise and evaluate barriers to digital trade as well as strategic guidance on instruments and approaches to tackle current and future impediments.

THE TRICK IS TO KNOW A BARRIER WHEN YOU SEE ONE

There are at least two reasons why addressing impediments to digital trade is a complex issue. First, the reliance on data flows and digital technologies gives rise to a wide range of new considerations that weigh upon trade policymaking – for example, how to operationalise privacy considerations in a system that effectively never forgets and enforcing non-discrimination policy when discrimination resides entirely in machine-learning processes. Second, as noted above, the international exchange of digital goods and services is but a small part of the growing domestic digital economy. The pertinent regulatory frameworks impinge upon trade policy or rather, trade policy ought to be consistent with, and be guided by, national priorities in these areas. Thus, in the context

3 The 'Digital Sector' is but one of several DCMS Sectors and therefore the associated services export figures constitute a very conservative lower bound. By comparison, exports from the 'Creative Industries' are given as £37.9 billion; it should be noted, though, that DCMS Sectors are not mutually exclusive and therefore these export statistics are additive to some degree but not entirely.

of digital trade, a conducive environment requires a concerted effort from across key areas of public policy, ranging from intellectual property rights, consumer protection, competition policy and cybersecurity to something as specific as a dedicated strategy on artificial intelligence.

Given the breadth and complexity of the subject area, no conference can be simultaneously comprehensive and comprehensible, so this one dealt only with a selection of topics. Half of the papers aim at identifying and codifying (some) barriers to digital trade, while the other half discuss the next logical step, which is ideas with the potential of dealing with these impediments. The focus is international rather than UK-specific, but the discussion of developments in other countries is undertaken with the explicit aim of inferring lessons for the UK as it devises its policies for ongoing and future trade negotiations.

Areas that are undoubtedly important but that were not considered in this inaugural conference include, for instance, the taxation of digital goods and services, anti-competitive behaviour by digital intermediary platforms, or an in-depth discussion of the value of data and how this may affect government policy. A discussion of some of the issues that are not part of this eBook can be found in Jones et al. (2021), who analyse in detail five areas of policymaking – including data flows and intellectual property – for digital trade in the UK.

Highlights from the individual papers at the conference are set out below. First, however, we make some general observations arising from more than one paper or from the discussions at the conference.

- Two recurring themes are digital trade's intrinsic link to cross-border data flows and the crucial role of property rights, including over software and data, in the process of formulating trade policy. Because artificial intelligence is a combination of software and data, this sweeping and rapidly evolving field is poised to have a major influence on digital trade policymaking.
- Barriers to digital trade may arise as readily from the *lack* of something – for example, a data governance framework – as from the existence of something inappropriate. Indeed, the judgement in the so-called '*Schrems II*' case has demonstrated that inadequate data protection laws can pose a significant barrier to the free flow of data.[4] Repositories of impediments to digital trade need to cover both state actions and inactions. This raises the deeper question of the identification and codification of best practice for digital trade governance. In this regard, digital trade is unlike 'regular' trade policy in which the impediments are mostly sins of commission.

4 Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems.

- Regulations pertinent to digital trade are spread over several branches of law, not always the obvious ones – for example, trade secrets, copyright, competition, security and human rights. Thus, while treating impediments to trade clearly requires addressing the locus and form of the regulations, determining priorities requires, rather, a focus on their effects. That is, it is a whole-of-government job.

- The characteristics of data imply that digital protectionism is more complex than 'conventional' protectionism. It may reside in near-trade or non-trade areas of policymaking such as investment screening with regard to data-rich firms (Aaronson 2020).[5] In addition, state actions or inaction in the areas of censorship, disinformation or algorithmic decision-making can constitute barriers to digital trade, and such actions have an added political or human rights dimension. As a result, trade policy can become charged with other sensitive policy areas.

- Given that the marginal cost of the electronic transmission of data and information is virtually zero, there is a huge public good aspect to regulating its flow. So why does it not flow freely?

- Part of the reason is that data and information are subject to strong network effects – the benefits of participation in their transfer are directly related to how many other parties participate. This encourages 'winner-takes-all' competition, which, coupled with the large differences in the underlying principles and values of the two major players (the US and China), tends to draw governments into commercial rivalries – and into actual and proxy trade wars on their respective producers' side.

- Following from this is the observation that one cannot get away from competition policy in the digital domain. Platform intermediaries take advantage of information asymmetries, have reached a size that levels them up with countries, and their concentration in just two economies has clear geospatial power implications. While the first step of addressing competition issues may lie in domestic regulation, the global scale of winner-takes-all markets renders it international. Depending on the exact problem to be addressed, there is a very strong case for ensuring, for example, the interoperability of different platforms or the portability of data, so that consumers can stimulate competition via easy switching.

- At the same time, governments need to protect individual rights such as privacy and other human rights, commercial secrets and the security of their networks. This will often require that governments have access to commercially sensitive information such as source code or data on the operations of providers, which in turn requires that commercial entities have confidence in the willingness and ability of governments

5 For instance, the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 requires that the US Treasury Department review foreign investment in new technologies, national security-related infrastructure and other areas.

to maintain legitimate confidentiality. The alternative of relying on the platform providers' home governments to enforce these rights worldwide would require very high levels of trust.

- It has proved hard enough to get agreement on most digital issues within 'coalitions of the willing' who have signed specific trade or digital economy agreements. Unsurprisingly, therefore, progress at the WTO has proved extremely slow, with the exception of the now mature, but threatened, moratorium on imposing customs duties on electronic transmissions. Because of the stalemate at the multilateral level, the compatibility of digital trade provisions and data governance frameworks across agreements with overlapping membership becomes a very pressing issue for trade policy in medium-sized economies such as the UK or Canada.
- Given the complexity of digital issues and the potential role that digital engagement can play in terms of development, a mechanism needs to be found to give developing countries, especially small and low-income ones, confidence that they will not be disadvantaged by the first-mover advantages of the major players. This is necessary in order that they do not block promising developments in international regulation.
- Medium-sized powers such as the UK have a strong interest in trying to devise international solutions. They are large enough to have stakes in at least some areas of digital trade, but not large enough to reap a full set of economies of scale or to impose their views upon the sector. Thus, either they have to choose sides or they need a common solution. The latter needs processes of cooperation, which probably require explicit creation and nurturing.

INSIGHTS ON MEASUREMENT AND EVALUATION OF IMPEDIMENTS TO DIGITAL TRADE

Evidence-based policymaking with regard to digital trade is a challenge not least because a comprehensive and continually updated repository of information on policy measures affecting digital trade does not currently exist. Such information would be hugely valuable for informing deliberations on the design, implementation and reform of relevant government interventions, on their cross-border effects, and on the potential for international cooperation. Addressing this deficiency has a conceptual, a practical, and a logistical dimension. Simon Evenett and Johannes Fritz (Chapter 1) explore how one could go about collecting meaningful information about policy stances towards digital trade. They summarise what can be learnt from three initiatives that have been undertaken to map trade-related aspects of the digital economy (ECIPE's Digital Trade Estimates, USTR's National Trade Estimates, and the OECD's Digital Services Trade Restrictiveness Index). They conclude that, between them, these three high-profile collections of information on digital trade policies do not provide a settled, common set of stylised facts to guide policymaking or analysis. Moreover, ECIPE's project is no longer updated.

Thus, Evenett and Fritz propose an attribute-based approach to information collection, whereby policy measures are described in terms of their attributes. Is the measure even-handed? Is it transparent? Does it allow scope for affected parties to engage the government over its consequences? And is it best practice? They advocate that every detailed entry in the repository should report on these attributes and hence be amenable for use in monitoring, benchmarking, and negotiations. These goals can only be usefully met if the attributes-based collection is maintained and extended over a number of years.

Notwithstanding a detailed plan about what, where, when, why and who should collect information, Evenett and Fritz acknowledge further conceptual challenges ahead, chief amongst which is the unresolved question of what ought to be regarded as best practice in governing digital trade. It is only against this ideal benchmark that impediments and deficiencies can be meaningfully identified. As was the case years ago with the World Bank's Doing Business database, there is currently no consensus on what best practice policy is, and it is also likely that it will be context-specific (for example, for countries at different stages of development). Hence, it may be advisable to list several best practices and make the repository searchable in that dimension.

Amongst the many different kinds of policies affecting digital trade, those governing cross-border data flows assume particular significance given the centrality of data flows to the digital economy: data enables the coordination of international production processes as part of global value chains, it helps small firms reach global markets, and it provides a conduit for delivering services. At the same time, a growing number of regulations condition the movement of data across borders in the wake of mounting concerns about privacy protection, digital security, intellectual property protection, and, in some instances, also industrial policy considerations. Thus, Javier López-González, Francesca Casalini and Taku Nemoto (Chapter 2) map the evolving regulatory landscape identifying how countries approach their cross-border data flow regulation and the different instruments they use to 'enable data transfers with trust.' They observe that the emerging patchwork of rules and regulations renders it difficult to effectively enforce public policy goals like privacy and personal data protection across different jurisdictions. It also increases costs for firms operating across different markets, potentially curtailing their ability to internationalise and to draw benefits from operating on a global scale.

By highlighting commonalities, complementarities and elements of convergence across different data governance instruments, López-González and his co-authors contribute to finding pathways towards greater interoperability between the emerging regimes. They find surprisingly many commonalities in plurilateral agreements, which belies the first impression of a maze of approaches; they note that these patterns may serve as building blocks for an international architecture on data flows, potentially under the aegis of the WTO's Joint Statement Initiative on E-Commerce. That said, the varied uses to which data may be put – from credit scores and Fitbits nowadays to unknown applications in the future – are behind the reluctance of countries and regulators to agree data-sharing mechanisms. Different regulatory remits further complicate the issue; for instance, the

sharing of financial data might be opposed by a regulatory agency that is tasked with preventing consumer discrimination, whereas it might be welcomed by another or part of the same regulatory agency if international data-sharing promoted financial stability. And for once, technological innovations can create more headaches than solutions. How can 'a right to be forgotten', as mandated in some jurisdictions, be enforced when data is stored with blockchain technology and therefore all stages entail all information?

Both these mappings refer to government interventions, or lack thereof, rather than to private sector actions and standards. The latter, too, may have implications for digital trade and/or the cross-border transfer of data, and should therefore certainly be within the purview of competition agencies and academic researchers. However, issues raised by private sector actions were not part of the brief for this conference.

Artificial intelligence (AI) represents such a sweeping and disruptive technology that the conference dedicated a chapter specifically to dissecting the legal issues for trade policymaking that arise from the proliferation of AI applications. AI makes use of other digital technologies such as cloud computing and the Internet of Things, which are themselves subject to (data governance) regulation. The growing ubiquity and interconnection of AI systems render its regulation and oversight extremely complex. Bryan Mercurio and Ronald Yu (Chapter 3) focus on the substantive issues that AI poses for intellectual property (IP) law and data governance, and specifically for provisions in these areas embedded in trade agreements. Thus, they identify links through which the UK's international trade strategy can influence success in the realm of AI.

First, because AI is a combination of software and data, access to data is paramount for market competitiveness due to the requirement of very large datasets to train AI systems. Compared to the US or China (or India, for that matter), the UK is a small market and will need to be able to obtain data to feed AI applications from abroad. This requirement would seem to be a powerful argument for securing free data flows. Equally crucial for feeding AI applications are 'text and data mining' (TDM) systems, yet these activities carry the constant danger of copyright infringements. One question for trade policy is whether the UK should develop an exception from copyright protection for AI database mining that functions across borders. Copyright issues not only loom on the 'input' side of AI but also figure on the output side – in terms, for example, of whether AI-created products (such as news articles) can/should be copyrighted and if so by whom. Here there are important differences even amongst jurisdictions that acknowledge copyright.

In the context of trade-offs that policymakers face, Mercurio and Yu's chapter makes a compelling case for cross-border data flows as a technological requirement. At the same time, though, this commercial need will have to be balanced with public policy objectives that may justify limitations, as elaborated by Teresa Scassa in Chapter 7. Similarly, since AI algorithms can be protected by IP instruments (such as copyright, patents or trade secrets) and some trade agreements provide for such protections, the UK will be an attractive location for AI businesses if the IP protection of its algorithms was

strong. At the same time, a wide range of public policy justifications exists for including provisions to require the disclosure of source code, as elucidated by a complementary in-depth discussion in Chapter 4.

The buoyancy of digital trade is underpinned in no small part by the fact that software is embedded in more and more products and services, and businesses rely increasingly on software-based tools to improve their operations, design products, set prices, or advertise goods and services. Software's expanding presence in internationally traded goods and services means that trade negotiators need to find a balance between encouraging software-based innovation and hedging against the risks inherent in the proliferation of software. Recent trade agreements incorporate specific provisions that prohibit governments and their agencies from requiring the transfer of, or access to, source code for applications that operate within their jurisdictions. Cosmina Dorobantu, Florian Ostmann and Christina Hitrova (Chapter 4) discuss how, on the one hand, these prohibitions can encourage international trade by reassuring foreign software developers that their product will remain protected. On the other hand, general prohibitions, even when accompanied by extensive exemptions, place limitations on the powers of governments and their agencies to examine source code for legitimate reasons. Dorobantu and her co-authors provide an excellent overview of possible motivations for government-mandated source code disclosure requirements, and they offer a detailed synopsis of all provisions related to source code disclosure across seven trade agreements concluded between 2015 and 2020, including the UK–EU Trade and Cooperation Agreement.[6]

They find that the exceptions to the general prohibition on requiring access to source code are comparatively narrow and do not cover the multitude of reasons why public authorities might legitimately want access to source code. Moreover, there is a tendency in recent agreements to expand the scope of the general prohibition on source code access to include algorithms. It is also notable that the enforcement of competition law, for instance, constitutes a legitimate exception to the disclosure prohibition in only two of the seven agreements examined (EU–Japan and EU–UK). Against the backdrop of the various reasons why public authorities might legitimately need access to source code, they recommend that trade negotiators give thorough consideration to, and exercise caution in, expanding the scope of the general prohibition on source code access to include algorithms. The UK–Japan agreement is innovative in that it allows for a broader set of actors to access source code for conformity assessment, which seems a useful development.

6 The US-Japan Digital Trade Agreement (2019), the United States-Mexico-Canada Agreement (2018), the EU-Japan Economic Partnership Agreement (2018), the EU-UK Trade and Cooperation Agreement (2020), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018), the Indonesia-Australia Comprehensive Economic Partnership Agreement (2020), the Japan-Mongolia Economic Partnership Agreement (2015) and the UK-EU Trade and Cooperation Agreement (2020).

DATA GOVERNANCE AND DIGITAL PROTECTIONISM

The first set of chapters has already foregrounded the centrality of data flows and their governance for digital trade to flourish. For instance, Chapter 3 gives a sense of just how much AI systems depend on access to personal and other proprietary data. Estimates suggest that the AI sector could add £630 billion to the UK economy by 2035 (Hall and Pesenti 2017) but the extent to which this potential growth will materialise is likely to hinge crucially on the prevailing data governance framework.

Hence, the second set of contributions revolves around approaches that address impediments to digital trade by facilitating access to, or the exchange of, data flows. This may or may not be linked to the negotiation of trade agreements. The EU has generally tried to keep data governance out of its trade agreements and to deal with it separately using equivalence decisions. However, the UK has now moved away from this approach and there are data flow provisions in both of its recent new trade agreements – with Japan (CEPA) and with the EU (TCA).[7] Data issues are therefore relevant for trade negotiations. And even if data governance was forged with different instruments, the question remains how current and future state actions around data and information might impinge on digital trade.

In her keynote address on the difficult past and troubled future of digital protectionism, Susan Ariel Aaronson (Chapter 5) starts from the opposite angle by observing that the world trading system has not yet found a way of handling governments' constant allegations that policy measures taken by other countries constitute a trade barrier to their digital economies. The transatlantic divide over whether or not privacy is protectionism, and whether the EU can achieve sovereignty over data and data infrastructure, provides a perfect illustration of the muddied debate over what is or is not digital protectionism. Aaronson argues that, going forward, policymakers need to adequately recognise the broad panoply of potential barriers to digital trade, including those that affect internet stability and trust (such as censorship or disinformation).

At its heart, digital protectionism differs from traditional protectionism because trade in data is unlike trade in goods or other services. Therefore, Aaronson defines 'digital protectionism' as referring to barriers to cross-border data flows and elaborates on the ensuing governance problems. Digital protectionism is different because there are many types of data; and because both data and the analysis of data can be a public good and can have huge ramifications for human rights. Moreover, many cross-border data flows are not directly affiliated with a transaction and they may not truly represent trade (which is the provision of a good or service across borders associated with an exchange of money). For these reasons, she acknowledges that there is no clear dividing line between

7 The so-called Continuity Trade Agreements, which roll over agreements with 66 of the 70 countries with which the UK had agreement via its membership of the EU, consciously aimed at not changing provisions negotiated with the EU, except where necessary for consistency or legal reasons. None of them makes advances in the digital realm.

legitimate and trade-distorting data governance. More dialogue and research are needed to establish what best practice data governance would look like, especially because a shared approach that promoted trust and interoperability would create a huge positive externality.

Recent trade agreements and most digital trade agreements cover only some of the potential barriers to data flows, including personal data protection, consumer regulation, spam, data localisation and source code performance requirements. Aaronson recommends further action with regard to these impediments that are already on trade policymakers' radars. First, a tightening of how and when nations can use the exceptions, whilst also recognising that practices such as the exploitation of psychological vulnerabilities for marketing purposes or for political manipulation could give rise to novel legitimate exceptions. Second, greater regulatory coherence and cooperation, particularly on disinformation and competition policies. Third, funding and building data regulatory capacity in the developing world.

Yet, the most important contribution of Aaronson's chapter may consist in its lucid discussion of the impediments to digital trade that most trade agreements do not currently address. These potential barriers to cross-border data flows encompass data-sharing rules, regulations on algorithmic decision making, competition policies, policies to limit disinformation, privacy labels for apps, censorship, internet shutdowns, and cybersecurity rules. In particular, Aaronson offers a detailed account of censorship and disinformation as trade barriers because, having additional implications for human rights and political integrity, they are particularly pernicious.

In the wake of Aaronson's keynote, two chapters further explore specific topics around data governance. Patrick Leblond (Chapter 6) asks what tangible progress for facilitating cross-border data flows could be made by drawing inspiration from the institutional setup of international financial standards-setting bodies. Although most recent trade agreements such as the Regional Comprehensive Economic Agreement (RCEP) and the United States–Mexico–Canada Agreement (USMCA) continue to include data flow provisions, his point of departure is that trade agreements are ineffective instruments for promoting digital trade, on account of the uncertainty associated with their provisions. Instead, Leblond argues that a superior solution would entail the creation of a separate, new international standards-setting body for governing data. This International Data Standards Board (IDSB) would be modelled on the best features found in existing international financial standard-setting bodies such as the Basel Committee on Banking Supervision, the International Organisation of Securities Commissions, or the International Accounting Standards Board.

Transposing the characteristics of these institutions to a new international data standards-setting body would permit its member nations to allow data to flow freely between them, because they would apply the same standards, in addition to cooperating closely in terms of developing those standards, sharing information and enforcing compliance. As a result,

member nations of the IDSB would form a single data area between them. In principle, if a large number of countries with different economic structures had been able to come together to develop, adopt and implement international financial regulatory standards, then one might think that there is no reason why the same could not be achieved for data – essentially, a plurilateral agreement of the willing. Yet the analogy has limits and may need adaptation; for instance, central banks as the financial regulators have always been in a strong position, which cannot be said for authorities that are currently tasked with data regulation. Moreover, as Aaronson's chapter shows, data flows have different characteristics from capital flows, and nations' engagement with the proposed IDSB would have to be consistent with both existing multilateral commitments and, perhaps more importantly, existing trade agreements, which currently follow different approaches to data governance.

Greater fungibility of data across jurisdictions can have enormous economic and social benefits; in particular, as pointed out by Mercurio and Yu, the burgeoning area of innovation from AI applications relies on vast quantities of data. The incentives for such benefits to materialise are strongest when data are protected as intellectual property, for example through copyright or trade secrets. The establishment of ownership rights imparts incentives to invest in data and allows businesses to appropriate the returns from such investments. In lockstep with this, however, the digital economy has stimulated an expanding public interest in access to data in a broadening range of contexts. This creates a tension between the legitimate scope for the protection of data and public interests that determine limitations on it. Teresa Scassa (Chapter 7) discusses how these competing interests could be balanced, noting that addressing public interest exceptions in the case of trade secret law may be particularly challenging.

The economic implications of this legal tension are far-reaching. As the digital and data economy expands, countries accumulate data with potentially high commercial value. In the context of health care, Israel has recently traded access to personal health information for Covid-19 vaccinations. Many nations have yet to determine how to manage their stores of data in the public interest purely domestically, even before contemplating trade agreements. Especially in the complex context of artificial intelligence, there is thus a risk that new provisions in digital trade agreements might strongly protect private interests in the confidentiality of data before the public interest in access to such data has had a chance to be articulated in domestic legislation. Hence, evolving trade negotiations should be attentive to the ways in which access to data, data transparency and data accountability may be required in order to appropriately govern artificial intelligence, protect human rights, and ensure goals of public safety and security. As such, Scassa's analysis provides important context to Mercurio and Yu's chapter on the requirements for an AI policy.

The conference concluded with an analysis of policy developments in the Asia-Pacific region, home to two of the most recent and most advanced agreements on digital trade. Whilst the biggest economies in the world are bogged down in competition and rivalry over regulatory approaches to data and digital protectionism, Stephanie Honey (Chapter 8)

explains how economies in Asia and the Pacific have quietly forged progress. Indeed, the Asia-Pacific region has consistently been at the forefront of digital trade policymaking, which has led to an overlapping web of ambitious digital trade provisions in regional free trade agreements. It has also spearheaded innovative 'digital-first' agreements that take a broad view of the digital economy and seek to create an enabling environment for digital trade.

These latter agreements, notably the open plurilateral Digital Economy Partnership Agreement (DEPA) involving New Zealand, Singapore and Chile, prioritise agility and collaboration in digital trade policy development. Their thrust is thus notably different from the conventional modus operandi of trade agreements, which, rather, typically define what governments may not do. But digital trade relies at least as much on proactive and ongoing regulatory cooperation as on a static list of prohibited interventions. As evidence of its success, Honey shows how DEPA has enabled interoperability in as sensitive an area as digital identities. The Digital Economy Agreement (DEA), between Australia and Singapore, seeks to encourage collaboration in areas such as AI, data innovation, digital identities, e-invoicing, trade facilitation or e-certification for agriculture.

Honey's contribution also emphasises the vital aspect of actively engaging with business stakeholders. Potentially in contrast to what governments or academics may think, it is worth bearing in mind that the private sector may have different perspectives or priorities on what constitutes a barrier to digital trade. In particular, businesses may be challenged by the emergence of a 'digital noodle bowl' of divergent trade rules. APEC and other regional integration initiatives have established consultation processes with the private sector. Such a model for trade policymaking is well suited to addressing impediments to evolving digital trade. The significance of DEA and DEPA can be seen as a demonstration to the global players of what can be achieved with creativity in digital policymaking. Moreover, DEPA is part of an 'open concerted plurilateralism' strategy and the agreement is thus poised to serve as a building block to multilateral approaches in the longer term.

CONCLUSION

It is difficult to overestimate either the challenges or the rewards in making sound international policy in the area of digital regulation and trade. The challenges clearly involve balancing interests at home and negotiating abroad; moreover, as the collective conference proceedings show, they also involve difficult technical and conceptual issues.

The chapters in this eBook point towards improved ways of collecting information on policies affecting digital trade. They elucidate linkages to other areas of law that are vital for digital trade policymaking, and they discuss the broad panoply of potential barriers to digital trade that might arise in the future. Going forward, a strong and varied intellectual work programme is the necessary precursor to solving the political and practical challenges. This eBook contributes to this effort.

REFERENCES

Aaronson, S (2020), "Data is Dangerous: Comparing the Risks that the United States, Canada and Germany See in Data Troves", CIGI Papers No. 241 (www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves).

Aaronson, S (2019), "What are we Talking About When We Talk about Digital Protectionism?", *World Trade Review* 18(4): 541-77.

DCMS – Department for Digital, Media, Culture and Sport (2021a), "DCMS Economic Estimates 2019: Gross Value Added", last updated 19 February 2021 (www.gov.uk/government/statistics/dcms-economic-estimates-2019-gross-value-added).

DCMS – Department for Digital, Media, Culture and Sport (2021b), "DCMS Sectors Economic Estimates 2019: Trade in services", updated 11 February 2021 (www.gov.uk/government/statistics/dcms-sectors-economic-estimates-2019-trade-in-services/dcms-sectors-economic-estimates-2019-trade-in-services).

DIT and DCMS – Departments for International Trade and for Digital, Culture, Media and Sport (2020) Understanding and measuring cross-border digital trade, Final Research Report (www.gov.uk/government/publications/understanding-and-measuring-cross-border-digital-trade).

Hall, W and J Pesenti (2017), "Growing the artificial intelligence industry in the UK", independent review (www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk).

Jones, E, B Kira, D B Garrido Alves and A Sands (2021), "The UK and digital trade: Which way forward?", Blavatnik School Working Paper BSG-WP-2021/038 (https://doi.org/10.35489/BSG-WP-2021/038).

ONS – Office for National Statistics (2021), "E-commerce and ICT activity, UK: 2019 – Use of information and communication technology (ICT) and the value of e-commerce activity by UK businesses", 5 February (www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/ecommerceandictactivity/2019).

Snower, D J and P Twomey (2020), "Humanistic Digital Governance", CESifo Working Paper No. 8792.

Wu, T (2006), "The World Trade Law of Censorship and Internet Filtering", *Chicago Journal of International Law* 7(1) (http://chicagounbound.uchicago.edu/cjil/vol7/iss1/12).

ABOUT THE AUTHORS

Ingo Borchert is a Senior Lecturer in Economics at the University of Sussex and Deputy Director of the UK Trade Policy Observatory. His research focuses on policies affecting services trade, and he has co-created the global "Services Trade Policy Database" published jointly by the World Bank and the WTO.

L Alan Winters is Professor of Economics at the University of Sussex, a CEPR Fellow and a Fellow and Founding Director of the UK Trade Policy Observatory.

CHAPTER 1

Mapping policies affecting digital trade

Simon J. Evenett and Johannes Fritz[1]
University of St. Gallen, St. Gallen Endowment for Prosperity through Trade and CEPR;
St. Gallen Endowment for Prosperity through Trade

1 INTRODUCTION

Digital technologies are transforming economies, social discourse, and political dynamics around the world. Commercial activity can be coordinated over much greater distances, allowing for much more fine-grained specialisation of tasks and spurring the development of cross-border supply chains. Opportunities to source from a wider range of suppliers have enhanced choice and created opportunities for entrepreneurs at home and abroad, widening the base of those gaining from international trade.

The social consequences of the spread of digital technologies have been profound too, a fact that has also influenced trade policy deliberation. Individuals and families can maintain ties much more easily than before, but some would argue at the cost of their privacy. New avenues for influencing and disrupting political campaigns have raised hard questions about the robustness of democratic processes. In many respects, these developments have been accelerated by the reactions to the COVID-19 pandemic, where digital technologies have fostered human interaction at a time when physical proximity has been strongly discouraged.

That the success of business models based on digital technologies is so uneven has inevitably linked the governance of digital technologies – at home, regionally, and globally – to national rivalries. Cross-border commerce facilitated by digital technologies has taken off while traditional trade and investment flows remains in the doldrums, further reinforcing the sense that some nations are winners and others losers from the spread of these general-purpose technologies. That a small number of large, high-profile firms are associated with these technologies combined with the perception that they operate in winner-takes-all markets motivates calls for a new round of regulation.

Unsurprisingly, then, these developments have not escaped the notice of policymakers, who seek to shape both the outcomes of such sustained and pervasive technological change as well as the organisations – both private and public sector – that are taking these

1 This chapter was presented at the CEPR-DCMS-UKTPO conference titled Addressing Impediments to Digital Trade on 1-2 March 2021, organised by the University of Sussex. We thankfully acknowledge questions from conference participants and comments from Ingo Borchert, Eric van der Marel, and Alan Winters.

developments forward (WTO 2020). With so many areas of law and regulation capable of influencing different aspects of digital technologies, government ministries and national and sub-national regulatory agencies often move at different speeds to enact and implement initiatives. It is far from evident that these initiatives have been coordinated, that much thinking beyond silos has occurred, and that policy is being grounded in the best available information.

A major problem in this respect is the lack of comprehensive accounts of the range of policies that affect the digital economy which can be meaningfully compared across jurisdictions. There are no accepted measures of digital trade policy stance, as there are in monetary policy for instance. Nor are there widely accepted outcome measures upon which to judge policy. It would be incorrect to assert that all policy towards the digital economy is being made 'on the hoof', or that policy deliberation is taking place in an empirical vacuum. However, when compared to the important task of macroeconomic management, policymakers seeking to shape the future course of the digital economy have little by way of qualitative and quantitative evidence to go on.

The past decade has seen industry associations,[2] international organisations,[3] research institutions and think tanks,[4] analysts,[5] and indeed some governments[6] assemble pertinent information on policies affecting the digital economy and, in a few cases, analyse their consequences. However, little by way of structured comparison of policy stance can be found to inform policymaking, and this largely reflects the large upfront and recurring costs of collecting information on the many different types of what are often referred to collectively as digital trade policies.

Officials often bemoan the lack of empirical evidence to guide and prioritise decision making but they rarely reflect on why this unsatisfactory situation has come to pass. That digital trade policies implicate many areas of economic law raises the entry barrier to data collection, in particular for individual scholars. In an era when datasets can be readily downloaded, unless there is the prospect of a massive academic breakthrough, few – if any – researchers have an incentive to devote the time to collecting large datasets. The opportunity cost is simply too great.

The career incentives of officials at international organisations tend to value quick wins over undertaking multi-year investments in forensic data collection. Many governments also withhold cooperation from the few information collection initiatives that public

2 See, for example, the reports and briefing of the Information Technology & Innovation Foundation available at https://itif.org/publications/reports-briefings.

3 The OECD has a work stream on public policies affecting electronic commerce, for example.

4 See, for example, the stream of analysis of related technological and innovation matters produced by the McKinsey Global Institute, available at www.mckinsey.com/mgi/our-research/technology-and-innovation.

5 Noteworthy papers on the trade-related aspects of policies affecting the digital economy are Aaronson (2019), Bauer et al. (2020), Chander (2014), Ferracane, Leendert, and van der Marel (2020), Meltzer (2019), and Mitchell and Mishra (2019).

6 Based it seems largely on industry inputs, the Office of the United States Trade Representative has expanded its coverage of so-called digital trade policies in their recent annual reports on foreign trade practices (see Section 3.2 of this chapter).

sector international organisations try to pull off. That many governments fail to back their fine words about the importance of policy transparency with resources to assemble information on digital trade policy choice also contributes to the dearth of reliable data. There are very good reasons for the under-supply of the global public good of transparency in digital trade policy.

The Digital Trade Estimates (DTE) project of the European Centre for International Political Economy (ECIPE) and the OECD's Digital Services Trade Restrictive Index (D-STRI) are notable exceptions although, as we argue later, their focus should be expanded to better meet the needs articulated by policymakers, civil society, and the business community. Indeed, in our view, some existing approaches to evidence collection on digital trade policies may have rushed too quickly to quantification before reflecting sufficiently on the very purpose of such information collection.

As is so often the case, the absence of a weak empirical base has not deterred trade negotiators from including provisions on electronic commerce in regional trading agreements. The Comprehensive Economic Partnership Agreement (CEPA) recently negotiated between Japan and the United Kingdom is a case in point.[7] Moreover, one of the so-called Joint Statement Initiatives being negotiated among a subset of the WTO membership relates to certain aspects of public policy that implicate electronic commerce.[8] Whether the provisions negotiated address the most important obstacles to digital trade is not a question that appears to faze trade negotiators.

The growing number of inter-governmental disputes over digital taxes and the like do not appear to be grounded in comprehensive assessments of what is at stake. In this respect, digital trade policymaking is probably no worse than other areas of trade policy – admittedly a weak test. Still, it is a far-cry from the gold standard of evidence-based policymaking, especially for commercial activities upon which many persons' livelihoods increasingly depend.

The premise of this chapter is that policymaking towards the digital economy, and towards digital trade in particular, would be improved if it were better grounded in evidence. Given many governments around the world are devising and revising policies towards the digital economy, an important part of that evidence base involves structured and meaningful comparisons of relevant public policies across jurisdictions. To that end, a cross-country mapping of pertinent laws, regulations, and their implementation needs to be developed and implemented in a rigorous and sustained manner. The central purpose of this chapter is to outline what such a mapping could involve, drawing upon the strengths and weaknesses of three high-profile attempts to track relevant policies that were, by and large, devised for other purposes.

7 For an official summary of the digital provisions of the CEPA, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/933990/uk-japan-cepa-digital-and-data-explainer.pdf.
8 Information on this initiative can be found at www.wto.org/english/news_e/archive_e/jsec_arc_e.htm.

The remainder of the chapter is organised as follows. The next section discusses why bother at all mapping policies affecting the digital economy. We argue that there are ten distinct compelling reasons, each of which can inform different aspects of policymaking. Then, in the third section, we discuss three high-profile initiatives to assemble information on policies affecting digital trade. We argue in the fourth section that attribute-based mappings will generate more policy-relevant information than the form-based mappings assembled to date. The fifth section of the chapter explains how such an attribute-based mapping could be implemented. Concluding remarks are presented in the final section of the chapter.

2 WHY MAP?

For the purpose of this chapter, we define a mapping of policies affecting digital trade as a structured, comprehensive, and meaningfully comparable set of information of the laws, regulations, and associated enforcement of a selected number of customs territories that implicate domestic and cross-border commercial transactions facilitated by digital technologies and other commercial activity that capitalises upon data acquisition, data storage, data processing, data analytics, and data transfer.[9] In this section we describe the many ways in which a properly executed mapping can contribute to policy formation processes, but first it will be useful to explain in more detail what a mapping is and what it is not.

Mappings differ from other ways to assemble information about policies affecting digital trade. A mapping goes beyond a listing of pertinent laws and regulations because it includes additional information about relevant aspects (dimensions) of those policy interventions. That additional information should be gathered by consistently applying a pre-specified and coherent methodology. Identification of the relevant aspects (dimensions) typically requires understanding both the broad class of legal regime in question as well as its potential consequences for other actors, in particular private sector actors.

A mapping differs from a case study in that the latter contains more narrative. Moreover, a mapping may provide useful inputs for the construction of a numerical index of policy stances towards digital trade but differs in that the latter involves making assumptions about the relative importance or impact of different policy interventions. However, a mapping can include assessments of the likely consequences of a policy intervention so long as those assessments are the outcome of the consistent application of a pre-specified and coherent methodology.

9 Digital value chains are said to comprise these elements, according to the 2020 edition of the WTO's World Trade Report (WTO 2020).

Proper mapping of policies affecting digital trade contributes to the:

1. identification of gaps in national policies towards the digital economy;
2. identification of other jurisdictions with similar, better, or worse policy stances towards the digital economy;
3. identification of changes in policy towards digital trade by foreign governments;
4. identification of emergent trends in policy stance of peer or rival jurisdictions;
5. identification and analysis of the determinants of differential policy choices across jurisdictions (triggers for policy intervention as well as root causes);
6. identification of better practice laws, regulations, and enforcement which, in addition to informing national policymaking, can be presented to relevant international fora, thereby contributing to a reputation for excellence in digital trade policy matters;
7. support for fact-based engagement with trading partners on policies affecting digital trade, bilaterally, regionally, in specialist fora, and at the WTO;
8. identification and/or development of provisions for inclusion in regional trade agreements and in plurilateral and multilateral trade accords;
9. identification of policy intervention taken by trading partners that contravene established international best practice or obligations of trade accords; and
10. structured inputs that can be employed in quantitative assessments of the impact of different types of digital trade policy regimes or in changing policy regimes over time.

Having described what a mapping is and its potential payoffs for the formulation of national policies towards the digital economy and digital trade, we turn to what policy interventions have been included to date in three publicly available compilations of information on relevant policy intervention.

3 INFORMATION COLLECTION INITIATIVES UNDERTAKEN TO DATE

We are not the first to advocate compiling information from many jurisdictions on policy changes implicating the digital economy. To identify similarities and our point of departure, in this section we describe the evidence collected in three high-profile monitoring initiatives on digital trade policy. We discuss the initiatives in order of vintage, with the newest approach discussed first.

3.1 The OECD's Digital Services Trade Restrictiveness Index

In his account, Ferencz (2019: 5) motivated the construction of this index as follows: "… little is known about the nature and extent of impediments that affect trade conducted through digital means". The OECD Secretariat's goal was to develop "an indicator that identifies, catalogues and quantifies regulatory barriers that affect trade in digitally enabled services" which could become "an evidence-based tool that helps to identify regulatory bottlenecks, design policies that foster more competitive and diversified markets for digital trade, and analyse the impact of policy reforms".

Although much effort was deployed in scoring policy interventions thought to affect digital services and in weighting them according to their likely impact so as, ultimately, to produce index values that are supposedly comparable across nations, when stripped to its core the informational content the D-STRI rests on evidence collected on 37 different types of policy intervention (see the list in Annex A of Ferencz 2019). Ferencz sorted these policy intervention types into the following five groups: "Infrastructure and connectivity," "Electronic transactions," "Payment systems", "Intellectual property rights", and "Other barriers affecting digitally enabled services".

Evidence collection by the OECD Secretariat began in 2014 on policy interventions by authorities in 44 (then 46) jurisdictions. Inevitably, some of policy interventions came into force before 2014. According to the relevant OECD website this database was updated to 2020 and covers digital trade policy measures affecting ten service sectors.[10] So as to facilitate comparison with the two other digital trade monitoring initiatives discussed in this section, from now on attention focuses on the policy interventions enacted or implemented since 1 January 2010. Information on all such policy interventions was extracted from the D-STRI database[11] and coded. As will become apparent, unfortunately, some entries in the OECD D-STRI database do not include the year of implementation.[12]

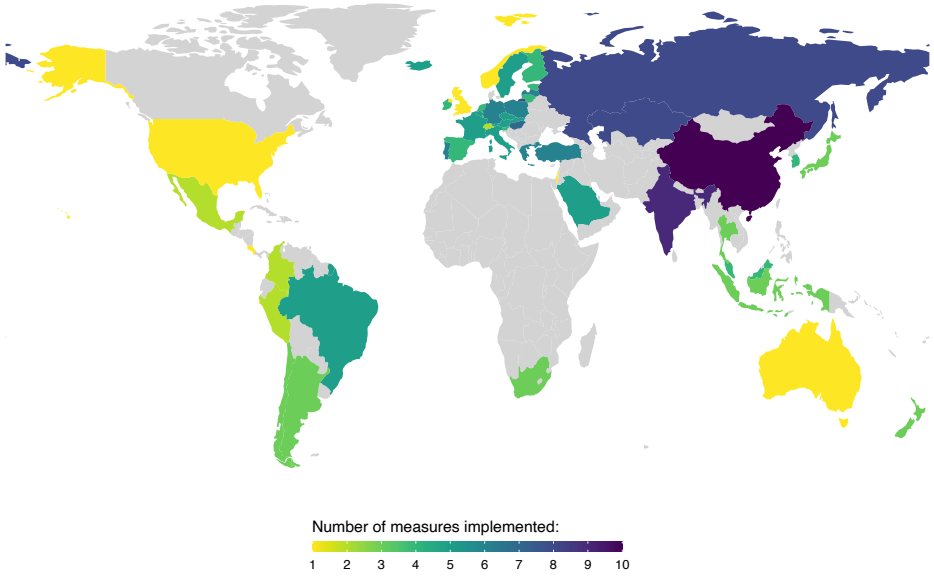
In terms of country coverage of policies enacted since 2010, the largest emerging markets and Western Europe accounted for a significant share of the 143 policy interventions found in the D-STRI database (see Figure 1). Fewer policy interventions were enacted in the English-speaking countries, it seems. Of course, counts of policy interventions have their limitations. One omnibus law covering many service sectors may have a more far-reaching effect than a series of sector-specific interventions. Still, China, India, and Russia stand out for the number of policy interventions affecting digital trade imposed during the years 2010–2020.

10 The ten service sectors are audiovisual services, computer services, construction services, courier services, distribution services, financial services, and logistics services, professional services (taken to be accounting, architecture, engineering, and legal services), telecommunication services, and transportation services.

11 For further information about that database, see https://qdd.oecd.org/subject.aspx?Subject=063bee63-475f-427c-8b50-c19bffa7392d.

12 Supplying information on the year in which a policy is implemented ought to be a basic requirement of a comprehensive mapping of digital trade policy.

FIGURE 1 FOR DIGITAL TRADE POLICIES IMPLEMENTED FROM 2010 TO 2020, THE BRICS AND WESTERN EUROPE ARE BETTER REPRESENTED IN THE OECD D-STRI THAN THE ENGLISH-SPEAKING MEMBERS.[13]



Source: Based on OECD Digital Service Trade Restrictiveness Index.

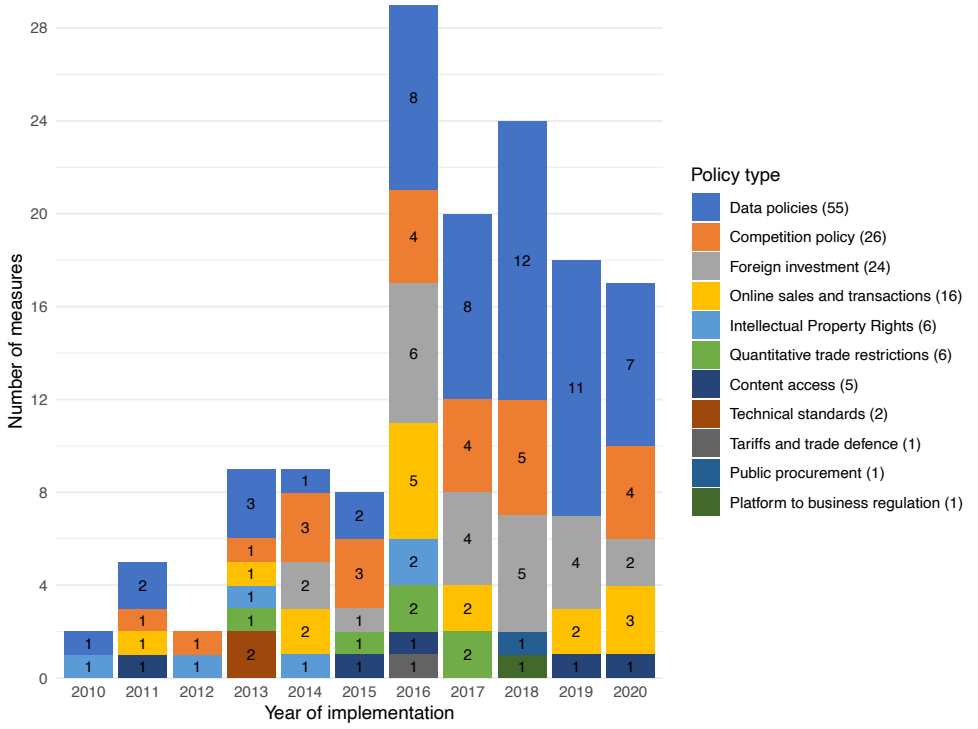
The 143 entries in the D-STRI that relate to digital trade policies enacted or implemented between 2010 and 2020 were then sorted into 13 types of policy intervention, chosen so as to facilitate comparability with the two other information collection initiatives summarised below.[14] It transpires that five-sixths of the entries in the D-STRI relate to four types of policy intervention: data policies, competition policy, foreign investment policy, and regulations concerning online sales and transactions (see Figure 2).

A total of 55 policy interventions relate to policies regulating the use, storage, and transfer of data alone. Resort to such data policies appears to have mushroomed during 2016 to 2020. More generally, resort to policies implicating digitally delivered services occurred twice to three times as often during the second half of the past decade as compared to the first half. If this picture is accurate, then it goes a long way to account for elevated private sector and government interest in digital trade policies.

13 It is telling that there is no information on digital trade policy changes for Canada since 1 January 2010. In fact, the D-STRI database does include one entry for Canada, relating to domain name registration. However, this entry does not include a year of implementation for the policy intervention in question. Further research revealed at that this policy intervention came into effect on 8 November 2000 (www.cira.ca/policy/rules-and-procedures/canadian-presence-requirements-registrants).

14 Eleven of the 13 types of policy intervention were found in the D-STRI database. See Table 1 in the next sub-section for a list of the 13 groups of policies implicating digital trade.

FIGURE 2 FOUR TYPES OF POLICY IMPLICATING DIGITAL TRADE ACCOUNT FOR 83% OF THE ENTRIES IN THE OECD D-STRI



Source: Based on OECD Digital Service Trade Restrictiveness Index.

3.2 ECIPE's Digital Trade Estimates project

The European Centre for International Political Economy (ECIPE) began an initiative to track restrictions on digital trade in 2017, naming it the Digital Trade Estimates (DTE) project. In accounts of this project, the emphasis was on digital trade restrictions as the following statement from their April 2018 report makes clear:

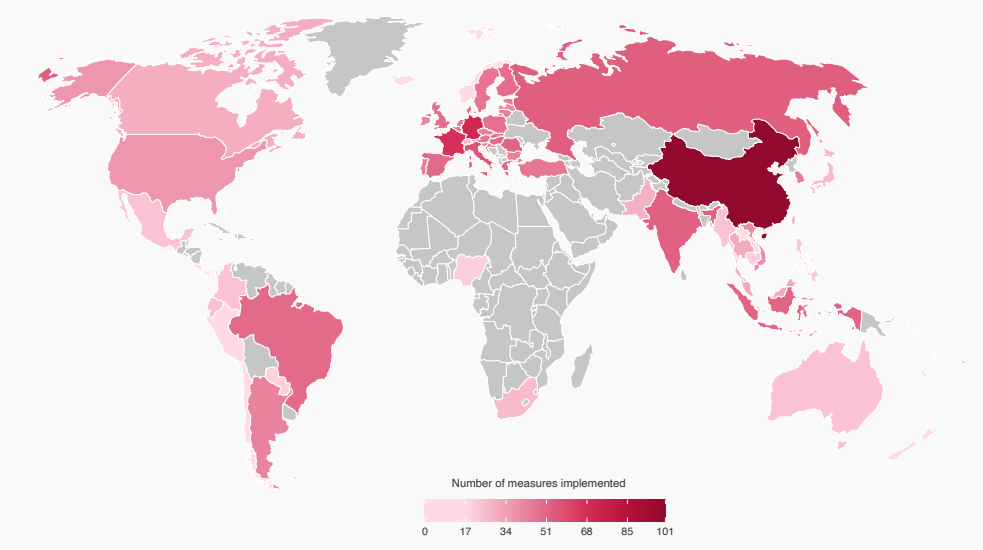
> "The Digital Trade Estimates (DTE) project sheds light on policy restrictions in the digital economy. More precisely, it is a source of information for policymakers, analysts and businesses who want a better overview on digital trade restrictions covering all aspects of the trade policy field" (ECIPE 2018: 10)

Information on policy interventions by the governments of 64 jurisdictions (counting the EU and each of its member states as separate jurisdictions) was collected going back in time, in some cases decades. This information was coded so as to construct a Digital Trade Restrictiveness Index (DTRI) from which it was possible to rank the 64 jurisdictions. By December 2017, the underlying database contained information on over 1,700 policy interventions (ECIPE 2018: 130).

A first insight from this ECIPE initiative concerns the geographic distribution of policy interventions affecting the digital economy (see Figure 3). By December 2017, policy changes affecting the digital economy were essentially a global phenomenon. A second is that, while all 64 economies tracked implemented some digital trade policies, the G20 economies undertook more policy changes – in particular, Brazil, China, India, Indonesia and the large European economies.

While many of the policy interventions that ECIPE collected information on refer to restrictions on either digital commercial transactions or the cross-border transfer of data that is a key part of many international companies' operating models, information on two other types of policy interventions was collected as well. The first are policies that affect private sector behaviour in the markets associated with the digital economy, an example being policies towards online sales and transactions, intermediate liability, and access to digital content. The second are policies that apply across digital and non-digital sectors of the economy (so-called horizontal measures), here information was collected on the enforcement of these laws to firms operating in the digital economy.

FIGURE 3 NUMBER OF NAMED POLICY INTERVENTIONS IN THE ECIPE DTE DATABASE



Source: ECIPE dataset.

Note: this information reported in this map refers to policy interventions named in the ECIPE DTE database and are not restricted to any range of implementation dates.

Overall, the ECIPE team collected information on 13 different types of policy intervention, organising them into four clusters (see Table 1), the titles of each of which refer to restrictions. Policies relating to the storage, use, and cross-border transfer of data are the most prevalent ones in the ECIPE DTE database where a specific, named policy act was

identified.[15] Policies implicating the conduct of online transactions are the second most prevalent group. Policies affecting foreign investments, access to public procurement contracts, and data-related aspects of intellectual property rights are each found between 170 and 190 times in the ECIPE DTE database. The five most prevalent types of policy interventions affecting the digital economy together account for 56% of entries in this database.

TABLE 1 ECIPE'S FORM-BASED MAPPING OF POLICIES AFFECTING DIGITAL TRADE: TOTALS FOR EACH CLASS OF POLICY INSTRUMENT

Cluster	Class of policy instrument	Number of distinct named dataset entries
Fiscal restrictions	Tariffs and trade defence	66
	Taxation and subsidies	110
	Public procurement	175
Establishment restrictions	Foreign investment restrictions	189
	Intellectual property rights	171
	Competition law	107
	Business mobility	133
Restrictions on data	Data policies	302
	Intermediate liability	91
	Content access	117
Trading restrictions	Quantitative trade restrictions	91
	Standards	75
	Online sales and transactions	209

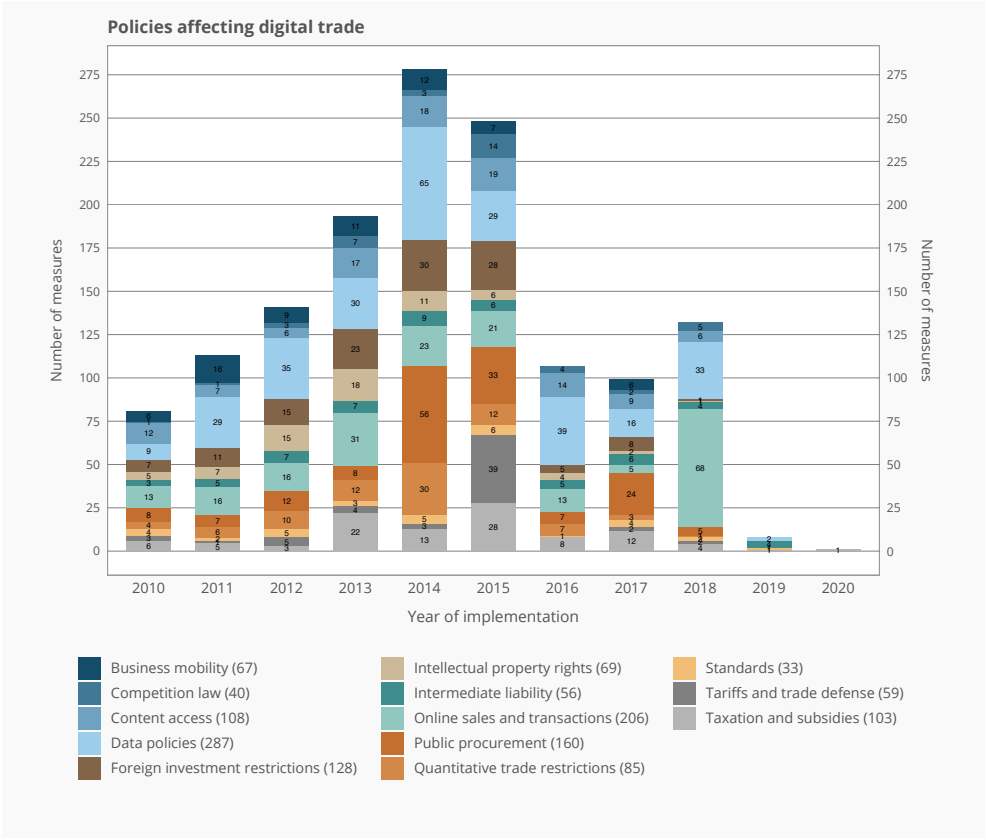
To focus on more recent policy interventions affecting the digital economy, we turn our attention to those state acts where the implementation date lies between 1 January 2010 and 31 December 2020. Figure 4 provides the annual breakdown by type of policy intervention of the state acts that came into force. Recall that this database was constructed in 2017 and 2018 and so the drop off in implemented interventions in 2019

15 The ECIPE database contains many unnamed or untitled policy interventions. The information recorded on the latter was too sparse to make consistent use of.

and 2020 is not surprising. To the extent that the ECIPE DTE database is a representative sample, then this suggests that the years 2013 to 2015 were particularly active years, with over 200 new policy interventions implemented in both 2014 and 2015.

During the years 2010 to 2020 a total of 287 new policy interventions relating to the use, transfer, and storage of data were introduced, with 65 such measures coming into force in 2014 alone. A total of 206 new policies implicating online transactions were also implemented since 2010, with 68 entering into force in 2018 alone. Public procurement measures implicating the digital economy were the third most frequently used policy tool, witnessed particularly often in 2014.

FIGURE 4 NUMBER OF DISTINCT, NAMED POLICY INTERVENTIONS RECORDED IN THE ECIPE DTE DATABASE WITH IMPLEMENTATION DATES FROM 2010 TO 2020, BY TYPE OF POLICY INTERVENTION



To the best of our knowledge, ECIPE's monitoring of policy interventions affecting digital trade has been discontinued. Consequently, two questions arise: Had monitoring continued and the database been updated, would the variation across time and across policy instruments remained broadly the same? And second, have other continuing policy monitoring initiatives confirmed the findings of this valuable ECIPE initiative?

3.2 Entries in the National Trade Estimates, 2015-2020

The annual publication by the Office of the United States Trade Representative of its *National Trade Estimates* is another source of information on digital trade policies. According to its latest (the 2020 edition) this report "highlights significant foreign barriers to U.S. exports, U.S. foreign direct investment, and U.S. electronic commerce" (USTR 2020: 1). This official report classifies foreign trade barriers into 11 categories, one of which is pertinent to this chapter:

> "Barriers to digital trade and electronic commerce (e.g., barriers to cross-border data flows, including data localization requirements, discriminatory practices affecting trade in digital products, restrictions on the provision of Internet-enabled services, and other restrictive technology requirements)" (USTR 2020: 2).

As to the sources of information on foreign trade barriers, the following quote reveals much emphasis is placed on information "compiled" by US Federal Departments:

> "The NTE Report is based upon information compiled within USTR, the Departments of Commerce and Agriculture, other U.S. Government agencies, and U.S. Embassies, as well as information provided by the public in response to a notice published in the Federal Register" (USTR 2020: 1).

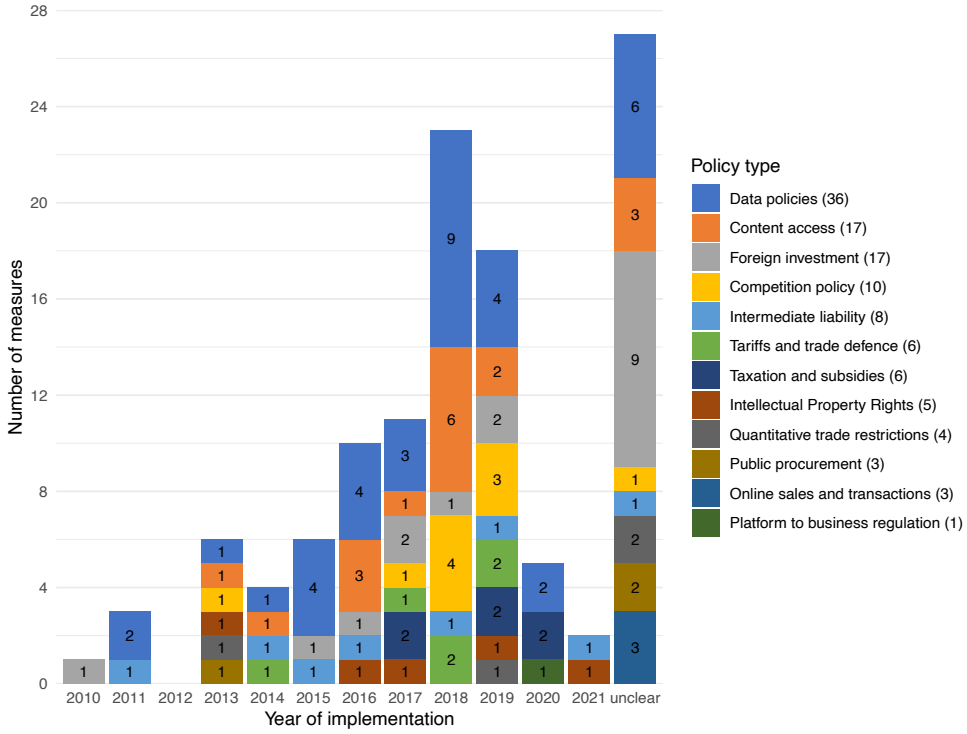
In reality, US companies with international operations and the business associations that represent them are said to bring alleged foreign barriers to the attention of US federal officials. These considerations need to be borne in mind when interpreting the picture of global digital trade policy painted by these US reports; it should be understood that the impression generated is largely one reflecting the concerns of influential US corporate interests.

Entries referring to digital trade or policies affecting the digital economy in the *National Trade Estimates* reports for the years 2015 to 2020 were compiled.[16] A total of 116 distinct entries relating to policy interventions implemented since 2010, or with no clear implementation date, were found and organized to the policy grouping used in the ECIPE DTE initiative. A total of 40 national governments were responsible for these barriers to US firms engaged in digital commerce.

16 It was difficult to find references to digital trade policies in the National Trade Estimates reports published in and before 2014.

Figure 5 provides the breakdown by year and by class of digital trade policy of the entries in the *National Trade Estimates* reports for 2015 to 2020. Like the OECD D-STRI, a number of entries in the *National Trade Estimates* reports do not mention the year of implementation (represented by the "Year unclear" column reported in Figure 5).

FIGURE 5 POLICY IMPEDIMENTS TO DIGITAL TRADE AS PORTRAYED IN THE US NATIONAL TRADE ESTIMATES REPORTS.



Source: Based on National Trade Estimate Reports on Foreign Trade Barriers (NTE) 2015-2020

Three important findings follow from studying Figure 5. First, through this lens, the number of foreign barriers to digital trade has tended to rise over time.[17] This finding must be interpreted with care.[18] It may well be that digital protectionism is on the rise

17 Reporting lags plus the fact that the 2020 ***National Trade Estimates*** report was published in April 2020 probably account for the small number of foreign trade barriers implemented in 2020.

18 Had widely accepted estimates of the annual totals of digital trade been available, then it would make sense to normalize the number of complaints to the US government in a given year by the relevant annual total for digital trade. This would reveal whether the total number of complaints (a possible proxy for the total number of actual digital trade impediments) rose at the same rate, faster, or slower than the total value of cross-border digital commerce. We thank one of the co-editors for suggesting this line of reasoning.

outside of the United States.[19] But it could also be that US companies are raising concerns about digital trade barriers more often.[20] And, of course, the use of digital technologies has been growing over time.

Second, three types of policy intervention account for 70 of the 116 entries on foreign barriers to digital trade. These are policies regulating the location, transfer, and use of data; policies conditioning user access to digital content; and state measures disadvantaging foreign investors and their operations. Clearly counts of foreign trade barriers need not reveal the quantum of harm to US commercial interests, but it is difficult to accept that the number of instances of such harm reveals nothing about the priorities of US firms that make the effort to raise these concerns with the federal government.

A third finding is that the number of competition policy-related state acts identified in the *National Trade Estimates* reports rose sharply in 2018 and 2019. If this is a taste of things to come, then a fourth category of foreign commercial policy may become a flashpoint between the United States and its trading partners. Overall, then, while in principle there are a wide range of public policies that could attract the ire of the US government or US companies operating abroad, in fact, at least as far as the *National Trade Estimates* reports are concerned, there are three – possibly four – policies which garner the most attention.

The picture painted in the *National Trade Estimates* reports is not entirely aligned with that found in the ECIPE and OECD information collection initiatives. For sure, policies towards the storage, processing, and transfer of data are the most common trade distortions in all three. However, measures affecting foreign investments by companies engaged in digital commercial activities and policies conditioning access to digital content account for a larger share of the foreign trade barriers found in the US reports as compared to the ECIPE dataset. Conversely, the latter contains a larger proportion of policy interventions relating to online sales and to public procurement policies. Competition law measures account for a larger proportion of the entries in the OECD D-STRI database than in the other two initiatives discussed here.

In conclusion, in general, these three high-profile collections of information on digital trade policy do not provide a common set of stylised facts to guide policymaking, analysts, or the private sector. (The exception being the prominence of regulations concerning data storage, use, etc.) This unsatisfactory state of affairs ought to be remedied by sustained independent monitoring of relevant policy developments. However, before that the purpose of such monitoring needs to be revisited, a point developed in the next section.

19 As these reports are silent on any barriers to digital trade erected by the United States, it could well be that digital protectionism as it is sometimes referred to is rising in the United States as well as in the rest of the world.

20 It may be worth reflecting on the factors that determine whether a firm brings to the attention of the US federal government information on a foreign trade barrier. For example, if US firms work on the assumption that their government is more likely to take steps that persuade foreign governments to remove digital trade barriers, then the rising number of reported foreign digital trade barriers need not reflect greater resort to digital protectionism abroad.

4 MAP WHAT? AN ATTRIBUTE-BASED APPROACH

All three approaches to collecting information on digital trade policies discussed in the last section have one feature in common – they are form-based. That is, information was collected on state acts falling within a pre-determined set of policy instruments deemed worthy of monitoring.[21]

One weakness with form-based approaches is that they are unlikely to catch new forms of policy intervention that influence digital trade. Indeed, a foreign government intent on protecting local commercial interests against foreign digital rivals might deliberately choose a form of policy intervention that is not on the list of those being monitored.[22] Form-based monitoring initiatives provide another rationale for substitution between trade policy instruments. This logic applies with as much force to digital trade policies as it does to trade policies of older vintage.

A different approach, which has proved to be both operational and revealing in the Global Trade Alert's decade-long monitoring of commercial policy, is to filter policy intervention based on their *attributes*. For example, if the policymaker's interest is in foreign commercial policy interventions that discriminate in favour of local firms, then monitors can sort through policy interventions according whether the implementation of a policy improves, worsens, or involves no change in the relative policy treatment of local firms vis-à-vis their direct foreign rivals.[23]

Attributes can be revealed in the formal statement of a law, associated implementing regulation, and in the subsequent enforcement of the law. Mappings could then include information on all three. For example, upon enactment a law may be classified as having a certain desirable attribute, whereas some subsequent enforcement action under that law may not.

With respect to digital trade policies the case for employing an attribute-based approach is stronger because there are – if the statements of governments, companies, and their business associations are anything to go by – probably even more attributes of interest. That a policy intervention discriminates is just one of the pertinent attributes calls into question the common practice of referring to all objectionable policies affecting digital trade as 'digital trade barriers'. A policy may not involve the erection of any specific impediment to digital trade, yet the implementation of the policy may still harm a foreign digital service provider, perhaps because the policy's implementation is not transparent and creates uncertainty for foreign market participants.

21 The WTO's monitoring of trade restrictions and trade reforms undertaken by the G20 nations is form-based as well.

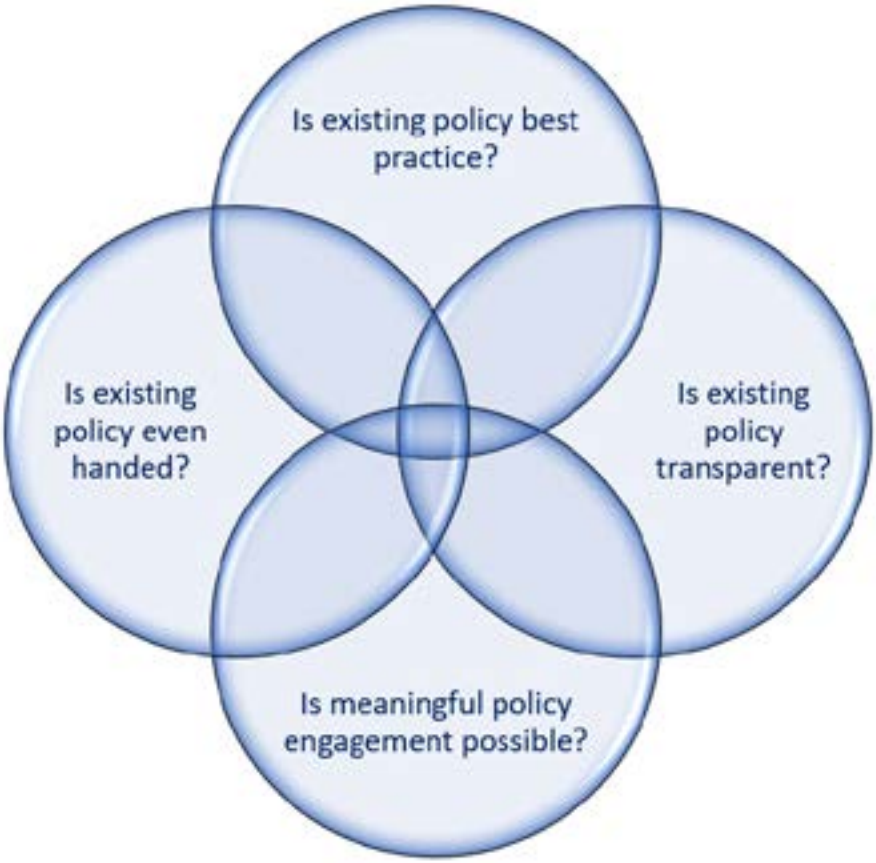
22 In the case of the United States National Trade Estimates report this argument only goes so far as nothing prevents US companies from bringing to the attention of the US governments new policies thought to constitute barriers to digital trade.

23 In the implementation of the Global Trade Alert this is referred to as the relative treatment test and aligns closely with the notion of discrimination developed in international trade law. For an account of the method used to classify policy intervention in the Global Trade Alert, see sections three and four of Evenett (2019).

On our reading of the position papers and statements about the policies affecting the digital commerce that seek to influence policymakers, there are at least four relevant attributes that a mapping of such policies ought to take into account (see Figure 6).

Starting from the left-hand side of the Venn diagram in Figure 6 is the question of whether a policy treats domestic and like foreign commercial interests in an even-handed manner. This is the matter of discrimination mentioned earlier, a classic concern of trade policymakers. On the opposite side of the Venn diagram is the question of whether the implementation of a policy intervention is sufficiently transparent. It has long been understood that the uncertainty engendered by a lack of transparency tends to depress cross-border commerce and the performance of foreign affiliates.

FIGURE 6 ATTRIBUTE-BASED MAPPING OF POLICIES AFFECTING DIGITAL TRADE



At the top of the Venn diagram is a matter of importance to foreign firms investing in or seeking to operate in a foreign jurisdiction. To what extent, if at all, does the set of policies that regulate the digital economy meet or conform to international best practice, in both design and execution? Taking this attribute seriously involves being open to the possibility

that a policy critical for the proper development of the digital economy is under-enforced or entirely missing. This is not a particularly new attribute of trade policy; some may recall that one oft-heard American complaint against the Japanese government in the 1980s and early 1990s was that the latter did not properly enforce its competition law. In the context of the digital economy, establishing competitive conditions and enforcing competition law are often said to be important in the telecommunications sector, irrespective of whether the incumbent firm is in the private sector or in the public sector.

The fourth attribute referred to occasionally in (largely) American commentary is whether there are opportunities to engage with foreign governments and regulators as new laws and regulations are being devised or revised. Since technological developments and business models in the digital economy are both evolving quickly, public policy changes may occur frequently.

Therefore, foreign companies and governments may seek to engage with those designing policy initiatives on the same terms as local businesses. They may also want to offer comments and suggestions on draft laws and regulations, much as companies do in the United States. This attribute, then, is about the engagement during the digital policy formation process and not about the state of existing policy and its implementation.

A trade ministry may be interested in one or more of these attributes. Once preferences over these attributes are known, which is tantamount to choosing a position in the Venn diagram in Figure 6, a mapping initiative should be designed accordingly. Official choice of pertinent attributes could be informed by expert advice as well as the legitimate concerns of the private sector. Those deploying the attributes approach should be open to the possibility that the number of pertinent attributes may change over time and that policymaker interest in certain attributes may wax or wane.

A policy intervention may meet or fall foul of a number of these attributes, allowing for a more nuanced assessment of policy interventions. Put differently, in the area of digital trade policies, determining whether a given policy intervention discriminates between domestic and foreign suppliers (the attribute of being even-handed) is one of several characteristics of potential interest to trade policymakers and affected stakeholders. This is not a novel proposition – not least to trade policy analysts, both legal and economic, that have studied traditional behind-the-border regulation.

In practical terms, looking at a policy intervention through the lens of these attributes has implications for the information that an analyst must collect, the questions they must ask, and the manner in which information on a particular policy intervention is enriched.

In classifying a policy intervention according to these attributes, the goal is to limit to the greatest degree possible the room for *judgement* calls by the classifier. Rather than judge whether a digital trade policy is a barrier or is protectionist, instead the analyst can judge

whether its de jure formulation would, if implemented, alter the relative treatment of domestic firms versus direct foreign rivals. In this manner, an explicitly stated standard would be consistently applied to assess whether a policy is even-handed.

Likewise, rather than judge whether a nation's policy is 'best practice', it would be preferable to follow the longstanding practice of identifying whether a national law or regulation states that it is aligned with, or takes as a reference, an accepted public global, regional, or sectoral standard.[24] Another approach here is to call out those national policy interventions that explicitly depart from an international standard. Moreover, in some cases, the absence of a law may constitute a departure from an international standard. In cases where there are competing international standards, then it will be useful to determine whether a particular national regulation meets the different facets of each standard.

Assessments of transparency can take as their starting point internationally accepted definitions of the relevant facets of transparency in a particular area of commercial law. Then national administrative practice can be benchmarked against those norms. For example, the International Competition Network, the club of national competition authorities, has guiding principles for procedural fairness in competition law enforcement which identifies several facets of transparent enforcement in the following statement:

> "Competition agencies should conduct enforcement matters under transparent rules and practices that provide parties under investigation with timely notice, as appropriate to the type of matter, that an investigation has been opened and its subject matter, agency concerns, allegations, and supporting evidence. Enforcement decisions should be transparent and explain the findings of fact, relevant legal and economic analysis, and any commitments or sanctions."[25]

The classifier would then check if the administrative practice of competition agency responsible for implementing a particular regulation affecting digital service provider has established procedures that fulfil every condition mentioned above (provision of timely notice, provision of information about allegations made, provision of supporting evidence, explanations of findings of fact, etc.) Such approaches are not new – they have been taken to assess many attributes of national merger policies and their implementation.[26]

24 In the case of voluntary standards adopted by private bodies that have been accepted by government, then the voluntary standard would be benchmarked against whatever international standards are the norm in the sector in question.

25 These Guidelines are available at https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/AEWG_GuidingPrinciples_ProFairness.pdf.

26 See, for example, https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/05/MWG_ImplementationRPsMergerNotification.pdf.

When applying the attributes approach to mapping digital trade policy, there are plenty of precedents in areas of commercial law to draw upon. Why? Because complaints about discriminatory, non-transparent practices implemented by regulators that do not follow international best practice and seal themselves off from engagement with foreign peers and the private sector are hardly new.

5 MAP WHAT?

What information would need to be collected if policymakers are to effectively track developments in the digital trade policy space? Keeping in mind the four attributes mentioned in the last section, we borrowed from the 'Five Ws' approach used in journalism, policing, and other areas of investigative work to formulate the following. To inform future digital trade policy choice, a mapping must include *what* was done *where*, *when*, *why* and by *whom*.

Translated into the policy monitoring domain for *announced unilateral policy changes* in digital trade policy, applying the Five W's and adding the reliability of the sources as an important sixth dimension leads us to propose collecting information on the following aspects of each policy intervention:

1. What?
    a. The **title** of the announced change including any official branding of it
    b. The **summary description** of the key elements of the change
    c. The type of **policy instrument** chosen, including a general nomenclature, where possible, to support connections to other datasets (e.g. the UN MAST classification for non-tariff barriers)
    d. Where relevant and feasible, the **direction of the change**, i.e. whether the commercial interests of the affected trading partners are harmed or benefit
    e. Where relevant and feasible, the **scale of the announced change** in its proper measurement unit (e.g. percentage change of a tariff or loan amount)
    f. The **type of economic activity** covered, including a general nomenclature, where possible, to support connections to other datasets:
        i. for physical products (e.g. the Harmonised System code)
        ii. for sectors including services (e.g. the United Nations CPC sectoral classification)
    g. The **commercial entities** covered, i.e. whether the change is firm-, location-, sector-specific or applies to all entities active therein
        i. If firm-specific, the **firm name**, location and other attributes, such as whether the firm or firms in question are state-owned (in whole or in part), state-linked, or otherwise state-controlled
        ii. If location-specific, the **location name** and other relevant attributes

h. The direction of the **primarily affected commercial flow** (e.g. inflows into an economy being distinguished from outflows)

2. Where?

   a. The **customs territory** where the public body announcing the policy intervention is located
   b. The **affected market**, which could include markets outside of the implementing jurisdiction
   c. The **trading partners** implicated by the implementation of the policy intervention

3. When?

   a. The **date** a policy intervention was **announced or updated**
   b. The **date** a policy intervention was **implemented or prolonged**
   c. The **date** a policy intervention was **removed** (if any)
   d. The **dates** during which any consultation period with the private sector, other stakeholders, and foreign governments is to be held or will be held
   e. The **date** the policy intervention in question was **documented** by the analyst

4. Why?

   a. The **purpose** of the policy intervention stated by the authority taking the action
   b. Whether the policy measure is said to be aligned with applicable **international best practices** or other **international standards**, technical and otherwise
   c. Whether the introduction of the policy measures was **justified at all**. If so:
      i. Whether the policy measure was justified on the grounds of **implementing an international accord** (such as a regional trade agreement) or whether the measure was taken pursuant to the rights a government has in an international accord (such as retaliation permitted following a WTO dispute settlement proceeding)
      ii. Whether the policy measure was justified on and makes specific reference to **scientific knowledge**
   d. **Related or precedent decisions** including policy intervention that has previously been announced (such as a national development strategy document) or changes made by foreign governments

5. Who?

   a. The **announcing agency** including whether it is a central government body, sub-national government body, independent state agency, state-owned or state-linked corporation or association, or supranational agency
   b. The **implementing agency** and its level/branch of government

   c. The agency that **reports** on any state action that is the result of the policy announcement, whether its reports are publicly available and the degree to which information is made available, and where those reports can be found

6. Information reliability?

   a. The reputation and independence of the data collector or provider
   b. The type of information sources used to spot the policy intervention
   c. The type of information source used to ascertain the above attributes of the policy intervention
   d. The official source, where available, including formal title of any associated law, regulation, etc.

That information on over 30 aspects of any one policy intervention can be collected indicates the considerable scope for enriching the information available to policymakers beyond assembling lists of policy announcements. Doing so requires a specially trained team. The resulting information would complement information on policy developments received from the private sector and from generalists posted to embassies abroad, the sources that many governments ministries tend to rely upon at present. In the highly politicised environment of our age, the reputation of the information assembler as a neutral, independent, and competent chronicler of policy choice cannot be overstated.

Some of the information identified in the "What?" sub-section above would allow for an assessment of whether policy change is even handed, liberalising, or discriminates against foreign commercial interests.[27] The information in the "Where?" sub-section helps identify the location of the affected commercial activity and the trading partners implicated. The information in the "When?" sub-section is useful in tracking policy stance over time and for assessing prior episodes of policy change. Information on the reporting agency facilitates assessments of the transparency of a particular policy initiative. Much of the other information collected is helpful in facilitating searches of a database for similar policy interventions[28] and in assessing the nature and quality of sources of information on policy change.

For *policy changes still being contemplated by a government*, so as to assess whether there are even-handed engagement opportunities for potentially affected commercial parties, information on consultation processes would be collected. This would include information on whether specific proposals are published in official registers or journals, whether there was a consultation process at all, whether comments can be submitted and under what timeframe, and whether there are other opportunities for engagement with decision makers.

27 Here, the relative treatment test mentioned earlier is relevant.
28 It being understood that seamless electronic access to policy intelligence is a desirable outcome. This is in marked contrast to the practice in some multinational corporations and trade ministries whereby mid-level officials hoard and become the guardians of information on policy developments.

In addition to mapping announced policy changes and announcements of policy reviews, which might be referred to as the flow of policy change, a full mapping should include information on existing policies that are likely to implicate digital trade as well as the absence of such policies. The latter two refer to, in the language of economics, the stock of current policy. This distinction is important for those designing mappings will need to choose whether to monitor the flow of new policy, document the stock of existing policy, or both.[29]

Implementing such a mapping of digital policy stance, and entering it into a database system that allows in real time for easy information extraction, for filtering according to user-selected criteria, and for intelligent aggregation, would represent a major improvement in the gathering and deployment of trade policy intelligence. For over a decade we have executed and refined such a mapping for traditional commercial policies (Evenett and Fritz 2020, Evenett 2019) and see no reason why a comparable mapping could not be created for policies implicating digital trade.

6 CONCLUDING REMARKS

In this chapter, having reviewed three inventories of policies affecting digital trade during the past decade, and having reflected on the questions of interest to trade policymakers, we have rejected form-based approaches in favour of an attribute-based approach. We went further to flesh out what such an attribute-based approach would involve in practical terms. Here we also reflect on the differences between the implementation of such an attribute-based approach in the digital trade space as compared to more traditional trade policies.

In traditional commercial policy monitoring, in general the absence of a policy choice is unnoteworthy. In the Global Trade Alert database, for example, no entries exist for tariffs that were not applied or subsidies that were not granted. In the digital domain, however, the absence of a policy choice may have a significant impact on market outcomes. For instance, the absence of user data protection regulation, intermediary liability, or copyright legislation are significant omissions in the policy toolkit affecting the digital economy. Comprehensive maps of the digital policy landscape thus must include the absence as well as presence of certain policy choices.

Traditional trade policy changes are also less prone to what might be referred to as directional ambiguity. It is seldom disputed that changes in import quotas, tariffs, and subsidies to import-competing firms affect the market access conditions of foreign suppliers of the goods in question. In contrast, the cross-border commercial effects of changing data protection legislation or user privacy rights may be harder to discern

29 So as to permit comparisons between the stock of existing policy (and non-policy) and the flow of new policy initiatives, to the extent sensible, the overlap in types of information collected should be maximised. In this respect, the 5Ws and the information reliability criteria listed above should be the starting point for developing a consistent set of characteristics collected on the stock of existing policy.

unambiguously. A comprehensive mapping of policies affecting the digital economy may not be able to draw, in every instance, conclusions about changes in the relative treatment of local firms and foreign rivals.

When it comes to adherence to international best practices and rules, there are closer parallels between more traditional forms of commerce and digital trade, in so far as the former are covered by unambiguous trade rules or other international norms.[30] Policymakers may also be interested in the extent to which a set of policies that regulate the digital economy meet or conform to international best practice, in both design and execution. Taking this attribute seriously also involves being open to the possibility that a policy critical for the proper development of the digital economy is under-enforced.

The approach advocated here should be seen in the context of longstanding arguments about the benefits of transparency in the world trading system. For some, sunlight is the best disinfectant, to quote US Supreme Court Justice Brandeis. For others, transparency serves the important role of putting pertinent facts on the table, thereby diminishing the role that fear and misinformation play in shaping the commercial relations between states. At a time of rising geopolitical rivalry, transparency initiatives that lower the temperature by supporting fact-based deliberation are valuable.

Another important trend to bear in mind is that, while many governments are not very keen on notifying international organisations of their policy changes thereby impairing that source of transparency, many of the same governments have embraced more transparent policymaking practices at home. More and more information is available on government websites and in official journals – and this information can be captured by digital means ('machines'). Even in its current deracinated state, the media still plays a useful role in highlighting when policy changes, when policy might change, and deficiencies in national policy, all of which are grist for the mill for those documenting digital trade policy stance.

These circumstances facilitate bottom-up, machine-driven information collection efforts on policy interventions affecting the digital economy and digital trade. However, for those efforts to be of greatest use to policymakers they must be carefully designed, implemented consistently, and executed for several years. Policymaking should be less informed by human-assembled inventories of policy intervention that are fraught with omissions, classification errors, and other biases. What is needed is the systematic enrichment of such inventories with pertinent characteristics of policy assembled in a meaningful manner that is readily accessible. The combination of trade policy expertise and machines should drag trade policy monitoring and deliberation into the 21st century – nothing less than a digitally facilitated approach for a digital era.

30 This is not to imply that mappings of traditional commercial policy must take a stance on, for example, WTO consistency of trade policy acts. In fact, at the Global Trade Alert, we took the view that we would not seek to duplicate or second-guess the operation of the WTO's dispute settlement understanding.

REFERENCES

Aaronson, S.(2019), "What are we talking about when we talk about digital protectionism?" *World Trade Review* 18(4): 541-577.

Bauer, M, M Ferracane, H Lee-Makiyama, and E van der Marel (2016), "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", ECIPE Policy Brief 03/2016, Brussels.

Chander, A (2014), "Data Nationalism", *Emory Law Journal* 3: 677-740.

European Centre for International Political Economy (ECIPE) (2018), Digital Trade Restrictiveness Index, Brussels (https://ecipe.org/dte/dte-report/).

Evenett, S (2019), "Protectionism, state discrimination, and international business since the onset of the Global Financial Crisis", *Journal of International Business Policy* 2(1): 9-36.

Evenett, S and J Fritz (2020), The GTA Handbook, Global Trade Alert, 14 July (www.globaltradealert.org/data_extraction).

Ferencz, J (2019), "The OECD Digital Services Trade Restrictiveness Index", OECD Trade Policy Papers No. 221.

Ferracane, M, E Leendert, and E van der Marel. (2020), "Digital Innovation in East Asia: Do Restrictive Data Policies Matter?", World Bank Policy Research Working Paper No. 9124.

Meltzer, J (2019), "Governing Digital Trade", *World Trade Review* 18(1): 23-48.

Mitchell, A and R Mishra (2020), "Data at the Docks: Modernizing International Trade Law for the Digital Economy", *Vanderbilt Journal of Entertainment & Technology Law* 4: 1073-1134.

USTR – US Trade Representative (2020), *2020 National Trade Estimate Report on Foreign Trade Barriers.*

WTO (2020), *World Trade Report 2020: Government policies to promote innovation in the digital age.*

ABOUT THE AUTHORS

Simon Evenett is Professor of International Trade and Economic Development at the University of St. Gallen, Switzerland. He is a Founder of the St. Gallen Endowment for Prosperity Through Trade, the new institution home of the Global Trade Alert initiative, the leading independent monitor of protectionism and commercial policy choice. Simon has written over 225 articles, book chapters, and volumes. He holds a Ph.D. in Economics from Yale University and a B.A. (Hons) in Economics from the University of Cambridge.

Johannes Fritz is CEO of the St.Gallen Endowment for Prosperity through Trade, the new institutional home of the Global Trade Alert. He holds a Ph.D. in economics from the University of St. Gallen, Switzerland, and works on the application of machine learning and computational text analysis methods to increase government transparency.

CHAPTER 2

Mapping approaches to cross-border data flows

Javier López-González, Francesca Casalini and Taku Nemoto[1]
OECD Trade and Agriculture Directorate

1 INTRODUCTION

In today's digitalised and globally interconnected world, data has become the lifeblood of our economic and social interactions. The proliferation of devices and sensors, the exponential growth in computing power, the plummeting costs of data storage, and the growing ability to deliver more data at greater speed have altered how we conduct our lives and how businesses operate (OECD 2020a). Whether for international trade (National Board of Trade Sweden 2014, MGI 2016, López González and Jouanjean 2017, Casalini and López González 2019), production (National Board of Trade Sweden 2015) or productivity (OECD 2015, Brynjolfsson and McElheran 2016), and in services (Ferracane and Van der Marel 2018), manufacturing (Brynjolfsson and McElheran 2019) and agriculture (OECD 2019), data – and its flow across borders – enable new opportunities to promote growth, wellbeing and inclusion (OECD 2015).

However, as we become increasingly reliant on data for our daily economic and social activities, new challenges have arisen. The growing exchange of data has fuelled concerns about the use, and especially the misuse, of data, amplifying concerns, among others, about privacy protection, digital security, intellectual property protection, regulatory reach, competition and industrial policy. This is especially the case when data cross different jurisdictions – the internet is global and borderless, but regulations are not.

As a result, countries have been adopting and adapting regulations addressing the movement of data, introducing measures that condition its movement across borders or, in some cases, measures that mandate that data is stored or processed in specific locations (Casalini and López González 2019). The resulting patchwork of rules and regulations is making it difficult not only to effectively enforce public policy goals like privacy and data protection across different jurisdictions, but also for firms to operate across markets, affecting their ability to internationalise and draw benefits from operating on a global scale.

1 This chapter draws on work undertaken in a range of studies by the authors, including Casalini and López González (2019) and OECD (2020a). The opinions expressed and arguments employed are those of the authors and do not represent the official views of the OECD or of its member countries.

Against this backdrop, the aim of this chapter is to provide an overview of the emerging policy landscape with a view to enabling more informed discussions on solutions that can enable the opportunities of digitalisation to be realised while tackling some of the new challenges it raises. This is an issue that has become more pressing in the context of an accelerated digital transformation resulting from the COVID-19 pandemic. Digitalisation has become key for mitigating the economic slowdown, sustaining wellbeing, and speeding up recovery (OECD 2020b).

2 WHAT IS DATA, HOW DOES IT FLOW AND HOW DO WE VALUE IT?

Global traffic from data centres is estimated to have increased fourfold since 2015 – from 5 zettabytes in 2015 to around 20 in 2021.[2] To put that into perspective, a zettabyte is 1,000,000,000,000,000,000,000 bytes (21 zeros) – that is, a thousand exabytes, a billion terabytes, or a trillion gigabytes. There are 20 times more bytes of traffic from data centres than there are stars in the expanding universe.[3] The pace of change shows no signs of slowing down; quite the opposite – global data flows are expected to continue growing at an accelerating pace (CISCO 2020), including after accelerated growth in bandwidth demand during the first wave of the COVID-19 pandemic (OECD 2020b).

However, the economic activity that growing data traffic supports is not easy to identify and measure. That is, how bits and bytes translate into dollars and cents is hard to establish. This is because, from an economics perspective, *data is different*. It is unlike other resources, factors of production, or inputs. First, data is valued at use, not at volume. For instance, a spreadsheet with 100 personal shopping entries may occupy the same memory space as one with 100 personal health records, but its underlying value will be different. A retailer will value the shopping entries more than a health service provider, which will value the personal health records more. The value of data is ultimately derived from its use, not its volume.

Second, the value of data can increase when merged to become greater than the sum of its parts. For instance, the shopping entries linked to the health records can help target advertisements towards the health conscious shopper. Third, data has both inherent and potential value. Information not used today can become valuable tomorrow with changing business dynamics or when combined with different data yet to become available.[4] Fourth, data can be copied at virtually no cost. This means that its use can serve many different

2 https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1908858

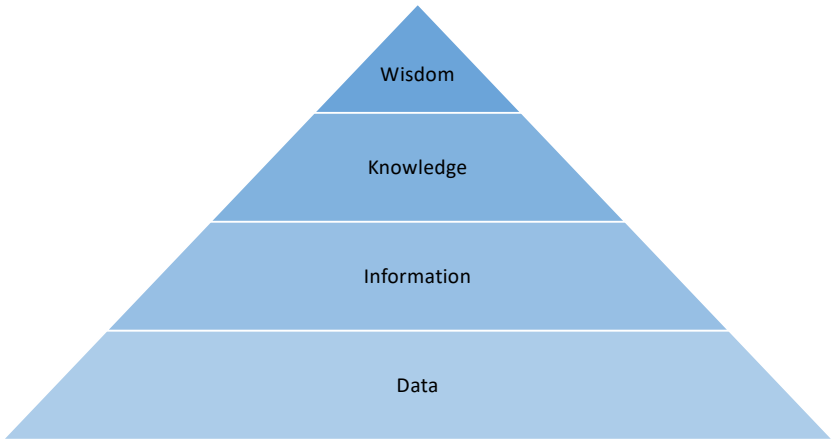
3 Based on data from the University of California, Santa Barbara accessed on 10 November 2020 (http://scienceline.ucsb.edu/getkey.php?key=3775#:~:text=The%20number%20of%20stars%20in,stars%20in%20the%20observable%20universe).

4 For instance, popular social networking platforms ran strong deficits during early years of operation while thinking about how to best capitalise on the mass of information gathered.

purposes at once.[5] The 100 personal health records may be used by one health service provider to research cures for cancer and by another to provide remote health services. The use for one purpose does not stop the use for the other (i.e. non-rivalrous).

This is why characterisation of data as the 'new oil' (Economist 2017) are misleading (Mandel 2017). Like oil, data is an essential input into the economy; however, data is not scarce and, as previously argued, it can be copied and transferred at virtually no cost. Ultimately, data are vast and unordered or unprocessed points that are collected; they become information when analysed to identify relationships between data points.[6] Knowledge is generated by analysts that recognise the importance of the information, and wisdom is generated by the decisions that make the most of the streams of analysed data. In this data–information–knowledge–wisdom (DIKW) hierarchy (Figure 1), each stage is dependent on those that come before it. There is no wisdom without knowledge, no knowledge without information, and no information without data.[7]

FIGURE 1 THERE IS NO WISDOM WITHOUT KNOWLEDGE, NO KNOWLEDGE WITHOUT INFORMATION, AND NO INFORMATION WITHOUT DATA



Source: Adapted from Rowley (2007).

Data also travels through the internet in *irregular ways*. When a file is sent from a computer in Country A to a recipient in Country B, it is first broken down into different 'packets'. These are like little parcels of information marked with the IP address of the sender, that of the recipient, and a code identifying the sequence in which the packets are to be reassembled at destination. Once the packets are ready, they leave the origin computer, crossing different networks and taking different routes to destination. Routers, the traffic wardens of the internet, guide the packets across networks, ensuring that, at

5 In economic terms, data might be thought of as non-rivalrous, which means that their consumption by one user does not prevent the simultaneous consumption by another.
6 Although there is a difference between data and information, this chapter uses these terms interchangeably.
7 This is a widely used model within the information and knowledge management literature.

each step, they take the shortest or least congested route. Once the packets arrive at destination, the computer assembles these according to their pre-specified sequence. If a packet is missing, a signal is sent for that packet to be re-sent.

This means that, when flowing between two countries, packets take different routes, often crossing different third countries. Moreover, the ultimate origin and destination of data flows is often a technical issue. Firms use mirror sites, which replicate webpages in different countries, to increase the speed of data transfers and also rely on cloud computing solutions which store different, and sometimes multiple, copies of files in different locations. This means, that, in some instances, what might seem to be a domestic transfer involves a cross-border flow (Casalini and López González 2019).[8]

3 DATA FLOWS MATTER FOR BUSINESSES AND CONSUMERS

The benefits of digital trade for both business and consumers are likely to be contingent on the degree of 'trust' that is placed on the activities of different players operating in the digital space. Individuals will not engage with businesses they do not 'trust', and businesses will struggle to reap the benefits of scale unless they can operate with 'trust' globally. From the perspective of consumers, concerns about data largely relate to how personal data is being used and the risks associated with misuse or theft of information. From the perspective of business, keeping data safe and enhancing trust remain top priorities, but concerns have emerged as to the impact of emerging data measures on the costs and ability to coordinate global value chains and engage in trade with some countries (Casalini and López González 2019).

3.1 Why are consumers concerned?

The information trail left in today's economic and social interactions is richer than ever before. For example, in the past, when renting a DVD, the information collected by firms would be limited to the name and address of the user and the titles and dates of collection and returns of rented films. Now, with digital streaming services, firms can also collect additional data on the time a particular movie was watched, whether it was finished or not, if it was watched multiple times, when it was paused, the extent to which it was enjoyed by the viewer (through ratings), and so forth. This information helps firms compile user profiles that can be used to make more targeted recommendations, improving service delivery.

This example also illustrates some emerging concerns – namely, that the amount of information gathered and the use made of it is not always clear to the consumer. With a growing online presence, more opportunities to record our activities arise, leading

8 The way data flows is often a technical matter contingent on how data is accessed and stored – whether through the cloud or using mirrors. This makes it difficult to identify the geography of data flows meaning that identifying whether a data flow is domestic or cross-border can also be challenging.

to a higher probability of revealing facets of ourselves that we may wish not to share with a company. This has fuelled growing concerns about privacy protection. Moreover, additional concerns arise when the data gathered is monetised in another form, such as by selling it to other firms who may make use of it for marketing or other purposes.

The control of personal information can affect the balance of economic power among different parties. For instance, a retailer holding information about an individual might be able to price discriminate, charging them a higher price than they otherwise would.[9] By contrast, if the consumer has the informational advantage, they might be able to get a nice bargain instead. In this case, information asymmetry can be redistributive (Posner 1981). At the same time, consumers benefit from sharing personal information, helping them reconnect with long-lost friends using social networks or through the use of 'free' software solutions for email, scheduling or navigation. The price of these services is often the personal data of the individuals, generated while the services are provided. All of this goes to show that the economics of privacy is ambiguous. Access free online services, but at the expense of less privacy. Reveal your preference about products so that you can get recommendations, but risk paying higher prices for goods in the future (Acquisty et al. 2016).

Privacy itself is also difficult to define. It means different things to different people (Solove 2006) and the value we attach to it, whether as individuals or in society, can be subjective (Acquisty et al. 2016).[10] This is also the reason why privacy protection differs across countries, reflecting different cultural and social traditions and norms. Owing to these differences, and to the fact that personal information is defined differently across countries, privacy and personal data protection is even more challenging when data cross jurisdictions.

3.2 Why are businesses concerned?

Today, firms across all sectors rely on data and cross-border data flows to support their business activities (National Board of Trade Sweden 2014, 2015). For instance, in manufacturing, data help to coordinate research and design outputs, exercise overarching control and coordination of geographically dispersed processes of production, and track and trace products as they travel to the border and beyond (Casalini and López González 2019). In agriculture, data is supporting a move towards precision agriculture techniques that rely on data analytics to optimise resources and enable savings on seed, fertiliser and irrigation, as well as allowing for new traceability and connections to markets (OECD 2019).

9 Indeed, if a firm is able to identify the consumer's willingness to pay for a certain product they can extract all consumer welfare replacing this with producer welfare.
10 Some also see privacy as a fundamental human right.

Firms also rely on data and its flow across borders at all stages of the value chain, from design to production, delivery and use (Figure 2). At the *design stage*, research and development for manufacturing activities increasingly involves coordinating individual researchers, scientists, designers and IT specialists working in different countries and sharing ideas, information, prototypes and test data.

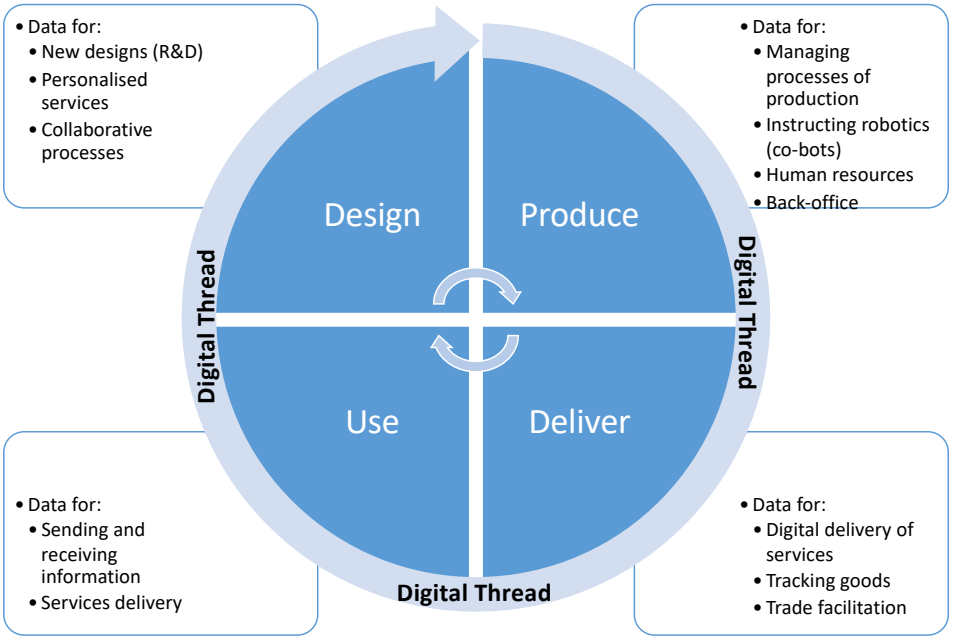
At the *production stage*, exercising overarching control and coordination of geographically dispersed processes of production also involves moving data across different locations: organising input flows of goods and services, working with subcontractors and suppliers, and handling internal operations. This requires, inter alia, sending data about inventories, sales, demand forecasts, order status, human resources and production schedules. As manufacturing becomes increasingly mechanised, data transfers are needed to instruct robotics. Sensors on the factory floor send real-time data that can be analysed and used to make necessary adjustment to production activities or equipment maintenance. Increasingly, this in-plant production can also require the transfer of data containing personal information of employees working alongside robots (so-called 'cobots').[11]

At the delivery stage, data transfers are needed to track and trace products as they travel to the border, across the border and beyond; data flows underpin modern trade facilitation practices (López González and Jouanjean 2017). Additionally, if the product being traded is a 'smart' good, the delivery of services and information – the elements that make the product 'smart' – will be contingent on the ability to collect and transfer different types of data. When the product gets to the consumer, at the use stage, the experience of the consumer might also depend on the ability of the firm to receive, process and respond to continuous feedback. Increasingly, firms also offer after-sales services, the efficient provision of which requires monitoring the performance of products in view of handling maintenance, repairs, and spare parts – again all connected through data flows.

All these elements, whether at the individual stages or taken as a whole, require constant digital connectivity via information and communication links supporting a 'digital thread' (Figure 2). Firms are concerned about measures that condition access to and use of these digital threads and how this might affect the efficacy of the individual stages as well as the viability of the value chain as a whole. Moreover, in the context of new technologies such as the wider adoption and use of the Internet of Things (IoT) or artificial intelligence (AI), reliance on data flows in production processes across both goods and services is expected to increase, amplifying existing concerns.

11 Indeed, in the case of agricultural supply chains, albeit with a different motivation, firms are increasingly sharing information with consumers about the persons engaged in the process of producing and delivering agricultural products in response to consumer demand to know more about how goods are produced.

FIGURE 2 DATA IS PERVASIVE ACROSS MODERN VALUE CHAINS



Source: Casalini and López González (2019).

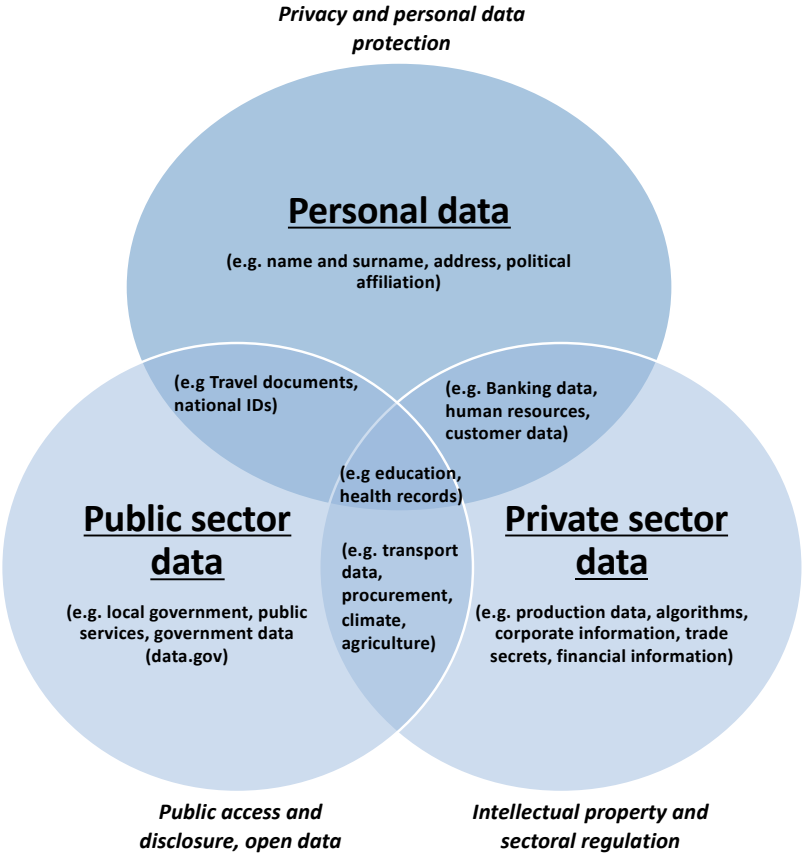
4 WHY IS DATA REGULATION EMERGING?

The growing and pervasive use and exchange of data, including across borders, has fuelled concerns about the use – and especially the misuse – of data, including in the context of power relations among firms and between firms and consumers, but in particular with respect to privacy and personal data protection. These concerns are compounded when data move beyond the reach of domestic regulatory bodies or is subject to differing regulations depending on where it is located and the type of information that it contains. Indeed, while data and digital activity are inherently borderless, regulations are not, and ensuring privacy and digital security, protecting intellectual property, enabling economic development and maintaining the reach and oversight of regulatory and audit bodies can become more complex when data cross jurisdictions.

Furthermore, different data are subject to different data governance frameworks. Personal data is subject to privacy and personal data protection but data from the private sector is generally subject to intellectual property rights (IPR) and specific sector-level regulations (as might be the case for banking or telecommunications data). Data related to the activities of governments and other public sector bodies are often subject to specific policies on access and disclosure. However, data types overlap, as is the case with publicly funded collection of personal data by private firms, raising issues that touch on different policy domains and data governance frameworks (Figure 3). In addition,

different definitions exist for different types of data. What one country might consider as personal data might not be considered as such in another (Casalini and López González 2019). All of this means that what data is subject to which data governance framework is a complex issue, with challenges compounded when data cross international borders where definitions, policy domains and data governance frameworks can differ.

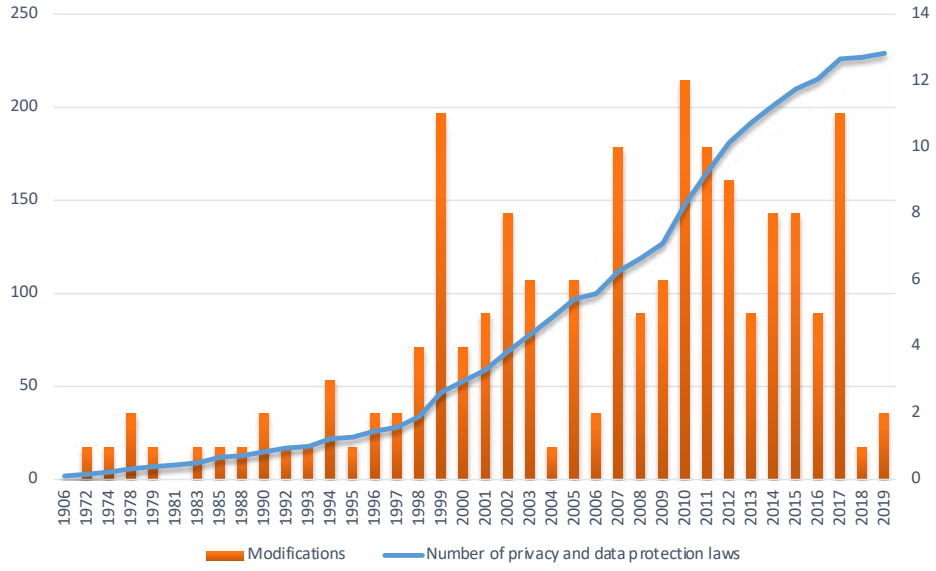
FIGURE 3 DATA TYPES AND DATA GOVERNANCE FRAMEWORKS



Source: Authors' elaboration.

In light of these emerging regulatory challenges, governments have been updating and adapting their data-related policies, resulting in a growing number of countries placing conditions on the transfer of data across borders or requiring that data is stored locally (Figure 4).

FIGURE 4 GROWING NUMBER OF DATA REGULATION



Note: Data regulations include different types of regulation relating to data transfers and local storage requirements. Numbers are affected by the way in which regulations are structured, as this varies by country – some countries may have a single regulation covering a wide range of measures; others will have several different regulations covering, for example, conditions on cross-border data flows for different types of data, and local storage requirements.

Source: Casalini and Lopez-Gonzalez (2019).

The reasons countries are reviewing their data policy are manifold, but can be broadly grouped into five categories (OECD 2020a). Much of the debate about data flows revolves around the movement of personally identifiable information, raising concerns about **privacy and data protection**. For some, the challenge is to ensure that, when data is transferred outside a specific jurisdiction, this data continue to receive the same protection that it received in the domestic jurisdiction. However, views on privacy and data protection can vary significantly across cultures, which is why regulation also differs.

Some measures that condition data flows aim to secure access to information for **regulatory control or audit purposes**. In this sense, requirements for data to be stored locally can be seen as the online equivalent of a longstanding practice in the offline world of ensuring that information is readily accessible to regulators. Such measures can be sector-specific, reflecting particular regulatory requirements and targeting specific data such as business accounts, telecoms or banking data.

Measures related to **national security** often mandate that data be stored and processed locally for the purpose of protecting information deemed to be sensitive, or securing the ability of national security services to access and review data. The latter in particular can be very broad in nature, providing wide scope of access to any form of data.

Governments also promote local storage and processing with a view to ensuring **digital security**. The rationale for implementing countries is that data security can best be guaranteed when storage and processing is domestic.

Finally, conditioning the flow of data or mandating that it be stored locally can be motivated by the desire to use a pool of data to encourage or help develop domestic capacity in digitally intensive sectors, a kind of **digital industrial policy**, including in the context of economic development. This can reflect the view that data is a resource that needs to be made available first and foremost to national producers or suppliers. These approaches can be sector-specific or apply to a range of data types.

Different motivations can lead to different measures on data flows, whether conditions on data flows or local storage requirements. However, in discussing these measures, it is important to consider the underlying policy objective for which they are applied. This can help in thinking through how effective the measures are in achieving their stated aims, the associated costs and trade-offs of such measures, and whether there are alternatives that would enable a better balance among different aims to maximise overall benefits for the population. From a trade policy perspective, these elements are relevant to identify whether a policy objective can be fulfilled in a way that is least trade-restrictive.

5 HOW ARE COUNTRIES REGULATING CROSS BORDER DATA FLOWS?

Domestic approaches to cross-border data flow regulation vary widely, reflecting different cultural preferences and policy objectives.[12] Amidst many differences, four 'types' of approaches have emerged (see Figure 4). These are not mutually exclusive; different approaches can apply to different types of data even within the same jurisdiction. For example, health data might be subject to more stringent approaches than data related to product maintenance.

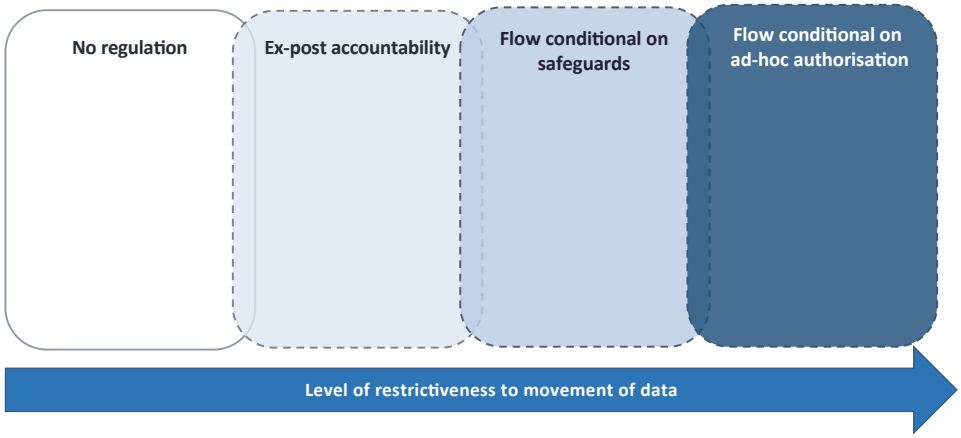
- At one extreme, in some jurisdictions (notably LDCs), there is **no regulation** of cross-border data flows, usually because there is no data protection legislation at all. While this implies no restrictions on the movement of data, the absence of regulation might affect the willingness of other countries to send data to these locations.
- The second type of approach does not prohibit the cross-border transfer of data nor does it require prior public authorisation or specific ex-ante conditions to be fulfilled, but provides for **ex-post accountability** for the data exporter if data sent abroad is misused (e.g. firms send data but if something goes wrong they are legally accountable).

12 Two broad types of data policies have emerged relating to cross-border data transfers: those that condition the movement of data across borders and those that mandate that data is stored locally (Casalini and López González 2019). This chapter focuses on the former.

- A third approach – **flows conditional on safeguards** – includes approaches relying on a range of pre-determined and transparent conditions for data transfer. In the context of privacy and personal data protection, these relate to determinations of adequacy or equivalence by a public authority. Where an adequacy determination has not yet been made, firms can move data under options such as binding corporate rules, or model or approved contractual clauses, among others.
- The last broad type of approach – flows conditional on **ad hoc authorisation** – relates to systems that only allow data to be transferred on a case-by-case basis subject to review and approval by relevant authorities. This approach relates to personal data for privacy reasons but also to more sweeping category of 'important data', including in the context of national security.

Across the different types of approaches, a number of exceptions are envisaged to permit the transfer of data. These include transfer in relation to 'legitimate interest' or in the 'public interest', or in relation to legal claims (among others). Data-subject consent is also a frequently used exception for permitting data transfers, but its use remains the subject of debate.

FIGURE 5 BROAD APPROACHES TO CROSS-BORDER DATA FLOW REGULATION



Source: Adapted from Casalini and Lopez-Gonzalez (2019).

6 WHAT INSTRUMENTS EXIST TO FACILITATE CROSS-BORDER DATA FLOWS?

While there are legitimate reasons for diversity in regulations, the regulatory landscape that underpins cross-border data flows is becoming increasingly complex. Moreover, the emerging patchwork of approaches risks undermining the different policy objectives they were intended to serve in the first place. Uncertainties about which rules apply to which data, resulting from overlapping or sometimes conflicting requirements for entities involved in data processing, can generate new risks. A firm that does not know what level

of protection it must afford to its customers or whether or not it can transfer some or most types of information across borders is going to struggle to ensure privacy protection and to engage in trade. At the same time, government enforcement action can also be hindered by a lack of coordination on these inherently transboundary issues. This, in turn, can undermine consumer trust.

Alleviating possible tensions between approaches and ensuring that data can flow with trust has been a goal of policy-makers for a number of years. Most recently, the concept of *data free flow with trust*, championed by Japan under the G20 'Osaka Track', encapsulates the idea that the benefits of digitalisation for trade and wellbeing depend strongly on the free flow of data and the degree of 'trust' in the digital environment. This was echoed at the G20 Riyhad Summit in November 2020, where leaders recognised the need to continue addressing challenges to "further facilitate data free flow and strengthen consumer and business trust". More specifically, the G20 Digital Economy Ministers highlighted the value of "identifying commonalities between existing approaches and instruments used to enable data to flow across borders with trust". Underscoring the need to promote further dialogue on instruments that can help bridge different domestic approaches.

Against this backdrop, governments and other stakeholders have increasingly been using a range of approaches to provide businesses with legal certainty as to the basis for data transfers while ensuring that, upon crossing a border, data is granted the desired degree of protection or oversight. Many different instruments and mechanisms have been devised and implemented; these can be grouped into four broad categories (Figure 6).

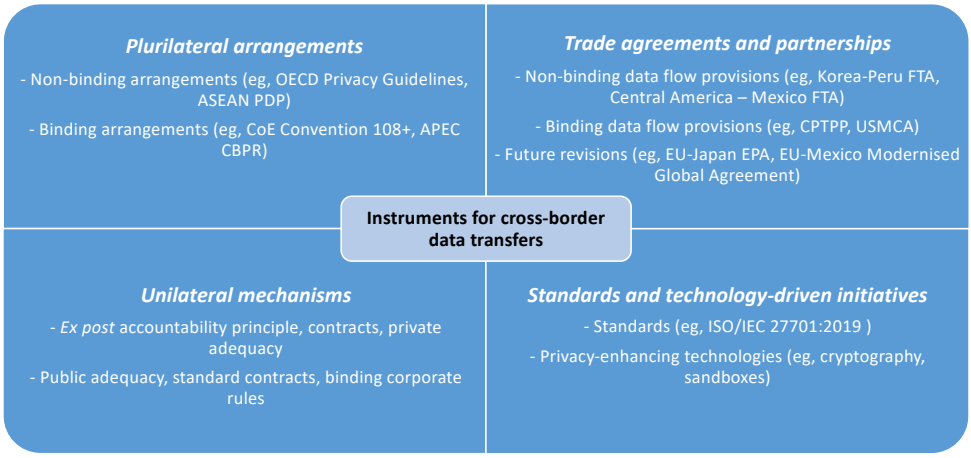
- **Unilateral mechanisms** enable the transfer of certain types of data to countries outside the domestic territory under certain conditions. They include the use of different mechanisms such as ex-post accountability principles, contracts, private sector adequacy as well as public adequacy decisions, standard or pre-approved contractual clauses and binding corporate rules. These transfer mechanisms are largely developed in the context of transfers of personal data.
- **Plurilateral arrangements** generate consensus around the transfer of specific types of data. The most well-known examples are in the field of privacy and personal data protection and include the OECD Privacy Guidelines, the APEC Cross Border Privacy Regime (CBPR) or the Council of Europe's Convention 108+.[13] There are many different approaches within this category, each with different levels of enforceability.
- **Trade agreements** are increasingly addressing issues around data flows. The depth and density of provisions varies from one agreement to another. For example, trade agreements such as the Comprehensive and Progressive Agreement for Trans-

13 Other examples of plurilateral arrangements might also include Interpol's Rules on the Processing of Data (RDP). These provide a framework for sharing data between 194 countries through the use of specific information systems.

Pacific Partnership (CPTPP) and USMCA or new types of digital trade arrangements (such as the Digital Economic Partnership Agreement between New Zealand, Singapore and Chile) provide binding principles on cross-border data transfers with enforcement mechanisms. At the same time, discussions on data flows are ongoing in the context of the Joint Statement Initiative on e-commerce at the WTO.

- Increasingly, access to data is being facilitated under **standard setting and technology-driven initiatives**. This includes the use of ISO standards and privacy-enhancing technologies (PET) such as cryptography technologies or data sandboxes that enable access to data within controlled environments.

FIGURE 6 INSTRUMENTS FOR FACILITATING CROSS-BORDER DATA TRANSFER



Source: Authors' elaboration.

Each broad instrument type tackles the issue of data transfers from a different perspective. The approaches are also not mutually exclusive – countries can use different approaches with respect to different partners, types of data and in different situations. The scope of data that each approach covers also varies. For instance, rules on cross-border data flows in trade agreements often cover all types of data, while existing plurilateral arrangements on cross-border data transfers, as well as some of the unilateral instruments, focus mainly on issues around privacy and data protection, areas where there has been most activity in the context of emerging regulation.

6.1 Unilateral mechanisms

Unilateral mechanisms are domestic approaches that enable the transfer of certain types of data to countries outside the domestic territory under certain conditions. A number of instruments emerge in this category, reflecting the tools through which the data policies in the typology shown in Figure 5 are implemented.

Ex-post accountability is where cross-border transfers take place without specific requirements such as additional legal steps. In these cases, 'trust' is placed on the data holder under the understanding that, if data is mishandled or misused in the foreign country, the data controller in the regulating country will be accountable – for instance, the US Privacy Act will remain relevant for US citizens if data is misused abroad. Another approach is where transferring entities are encouraged or required to develop their own legal instruments to protect the data when it crosses borders, such as through the use of *contracts*. Another approach is when the data holder is accountable for assessing the adequacy of the transfer (*private sector adequacy)*, often on the basis of principles indicated by the public sector. For instance, in Australia, transfers are permitted provided that the transferring entity "take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles". These approaches have in common that they do not need to be approved ex-ante by a public body. Although these types of rules are most often explicitly found in the context of privacy protection of personal data, they potentially apply to all data for which there are domestic rules but no specific rule on cross-border transfers (IPRs, confidentiality, etc).

Public adequacy decisions are unilateral recognition by a public body certifying that the personal data protection regime of another jurisdiction meets a certain level of privacy requirements and so personal data can be transferred unimpeded to that jurisdiction. A designated public body is in charge of determining adequacy or equivalence on the basis that the protection afforded to individuals in the receiving country is similar to that afforded domestically. This is the case, for example, for the European Commission's (EC) determination that Israel provides an adequate degree of privacy protection or the designation by the Colombian Superintendence of Industry and Commerce (SIC) that the United States provides adequate protection. The recently invalidated Privacy Shield Framework between the US and the EU was another example of an adequacy decision.

Ex-ante legal safeguards are instruments – sometimes used as an alternative where a public adequacy decision has not been made – that create, ex-ante, legal guarantees with regard to the transferred data, aiming to ensure uniform levels of protection and enforcement in the jurisdiction of destination. These unilateral instruments range from standardised contractual safeguards to binding corporate rules. Standard contractual clauses (SCCs) refer to ready-made rules that provide for personal data transfers to third parties located in other countries. The clauses, designed to be incorporated into contracts, are developed by data protection authorities (DPAs) and, as such, are considered to provide sufficient safeguards for the transfer of data, even to countries that do not enjoy an equivalence or adequacy recognition.[14] In turn, *binding corporate rules* (BCRs) bind the affiliates of a multinational company located in different countries to apply effective rights and legal remedies for the protection of personal data. These rules, once approved

14 Although, in some cases, the entities operating the transfer will still need to conduct a contextual risk assessment to ensure that the level of protection established by those standard contractual clauses can be respected in the destination country (that includes, for example, ensuring that there are no conflicts with the law of that country).

by the designated public body, enable data to move between affiliates located in different countries, even when these are in countries that do not recognise each other's data protection systems. Transfers are, however, restricted to affiliates within the group, and might be subject to risk assessment.[15]

6.2 Plurilateral arrangements

Plurilateral arrangements are international instruments that create rules, or aim to generate consensus, around cross-border transfers of specific types of data, often on the basis of alignment on underlying principles. The most widely discussed are those developed in the context of privacy and data protection.[16] These arrangements have often emerged under the auspices of regional organisations, but may also be open to participation by other countries (see Annex Table 1). Since they provide principles on privacy and data protection and cross-border transfers, they often go hand-in-hand with the unilateral instruments discussed in the previous section.

There are many different approaches within this category, each with different levels of enforceability. On one side, there are **non-binding plurilateral arrangements** that rely on 'soft law' to encourage parties to adopt data protection principles and promote interoperability between privacy protection regimes in order for data to be transferred between them seamlessly. An example of this is the 1980 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines"), which were revised in 2013 and set out guiding principles to ensure the protection of privacy while avoiding restrictions on data flows that are disproportionate to the risks presented.[17]

A regional example of a non-binding plurilateral approach is the ASEAN Framework on Personal Data Protection (ASEAN PDP Framework), which sets out principles of personal data protection for ASEAN member states to implement in their domestic laws. In 2018, building on the ASEAN PDP Framework, the ASEAN Framework on Digital Data Governance was endorsed. This framework sets out strategic priorities, principles and initiatives to guide ASEAN member states in their policy and regulatory approaches towards digital data governance, including for cross-border flows of all types of data (see Annex Table 1 for participating economies). ECOWAS and the Organization of Ibero-American States (in the context of the Ibero-American Data Protection Network) also

15 The DPA validating a set of BCRs may also need to conduct a risk assessment about the context of the operations.

16 However, other plurilateral arrangements, in particular to share a specific type of data among government agencies, exist across different fields. For instance, Interpol has developed specific Rules on the Processing of Data which include legal instruments with a global scope for regulating international exchange of criminal data. Similar agreements can be found in the context of passenger data exchange under the auspices of IATA.

17 The OECD Privacy Guidelines were the first internationally agreed-upon set of privacy principles on the protection of personal data whether in the public or private sector. They continue to be implemented by countries through legislation, enforcement and policy measures, and have influenced developments in privacy law, principle and practice in OECD countries and beyond. A growing number of countries have introduced privacy legislation in recent years, with many aligned with plurilateral arrangements such as the OECD Privacy Guidelines and the APEC Privacy Framework.

developed standards in this field, with the Supplementary Act A/SA. 1/01/10 on Personal Data Protection[18] of 2010, and the Standards for Personal Data Protection for Ibero-American States[19] of 2017, respectively.

There are also **binding plurilateral approaches** with stronger enforcement mechanisms. For instance, the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, commonly referred to as Convention 108 of the Council of Europe, is a binding treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. To date, 55 states have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions (see Annex A Table 1 for participating economies). The 2018 Amending Protocol, when it enters into force, will update the provisions on the flow of personal data between signatories (creating what is commonly known as Convention 108+).

The APEC Cross-Border Privacy Rules (CBPR) System, in place since 2011, also has a binding element, although it operates very differently.[20] The CBPR System is a government-backed data privacy certification framework that companies can join to demonstrate compliance with agreed privacy protection principles and enforcement mechanisms, allowing them to transfer data between CBPR participating economies with greater trust.[21] The CBPR System is not mandatory for APEC economies, and even when an economy adheres to it, companies can choose whether to seek certification under the System. However, once a company acquires the CBPR certification, it assumes liability under the CBPR framework vis-á-vis participating economies.[22] To date, nine economies have participated to the APEC CBPR system, four of which have accredited certification bodies, and around 30 companies have acquired the CBPR certifications (see Annex A Table 1 for participating economies).[23]

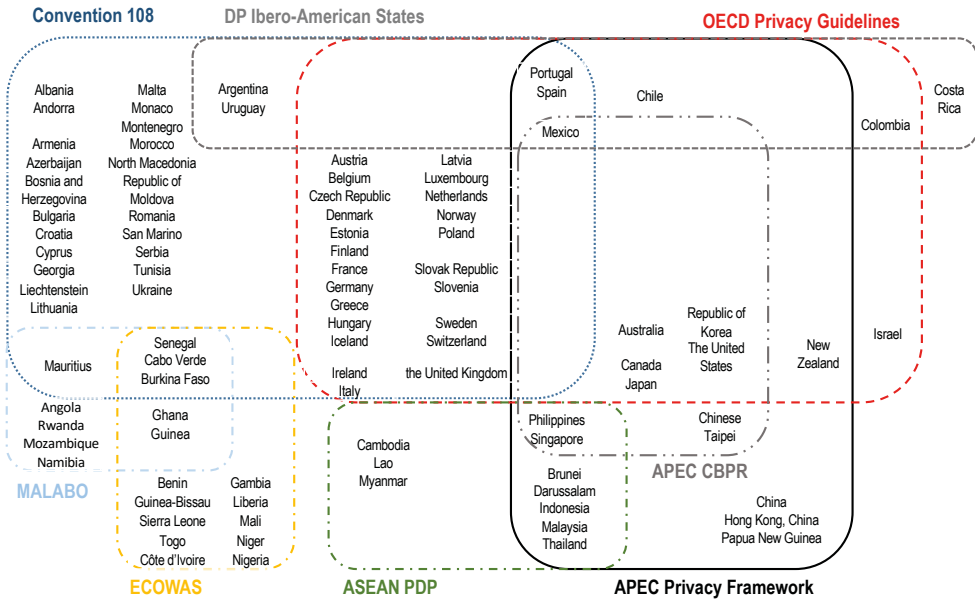
Another example of such an instrument is the 2014 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).[24] The Convention includes principles on personal data protection, and targets the protection of privacy without

18 https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf
19 https://iapp.org/media/pdf/resource_center/Ibero-Am_standards.pdf
20 The current version of the Framework (2015) draws upon concepts introduced into the OECD Guidelines (2013) with due consideration for the different legal features and context of the APEC region.
21 The APEC CBPR System requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework, a principles-based model for national privacy laws that encourages the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region. The APEC Privacy Framework was first endorsed in 2005 and updated in 2015.
22 Non-compliance may result in loss of CBPR certification, referral to the relevant government enforcement authority and penalties.
23 www.cbprs.com.
24 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

prejudice to the principle of free flow of personal data. To date, 14 countries have signed the Convention and eight countries have ratified it (ratification of 15 countries is required for the Convention to enter into force; see Annex A Table 1 for participating economies).[25]

The emerging landscape of plurilateral arrangements is therefore complex and has a number of overlapping memberships including at least 96 economies (Figure 7).[26] The common processes or principles that arise in the context of these arrangements are generally translated into domestic legislation. In this sense, plurilateral arrangements can promote the adoption of common privacy and data protection principles and reduce uncertainties related to the degree of protection afforded to individuals when data is moved across different jurisdictions, although causation can run the other way, with like-minded countries self-selecting into different arrangements.

FIGURE 7 THE OVERLAPPING MEMBERSHIPS OF PLURILATERAL ARRANGEMENTS



Source: Authors' elaboration

6.3 Trade agreements

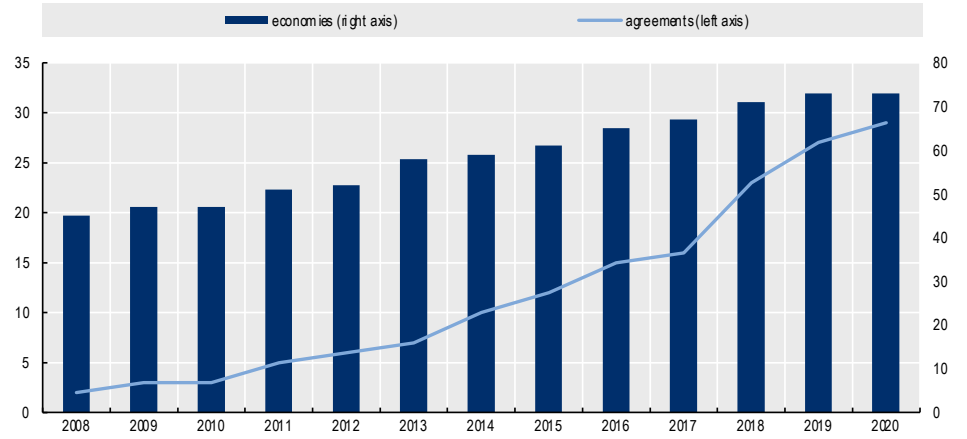
WTO agreements such as the General Agreement on Trade in Services (GATS) and the General Agreement on Tariffs and Trade (GATT) have bearing on data flows, as data measures may impact trade in goods, goods with embodied or embedded services and digitally enabled services. However, assessing the legality of measures on data can be

25 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

26 It can be difficult to count the amount of countries relying on the OECD Privacy Guidelines. Here, only OECD countries are counted despite there being wide evidence that the adoption of OECD Privacy Guidelines is more widespread.

complex (OECD 2019). While there are ongoing discussions at the WTO on specific e-commerce issues that include data flows, progress has been slow and cross-border data flows are increasingly being addressed in regional trade agreements (RTAs). Indeed, the Trade Agreements Provisions on Electronic-commerce and Data (TAPED) database (Burri and Polanco Lazo 2019) shows that, since 2008, 73 economies have signed provisions on data flows across 29 agreements (Figure 8).

FIGURE 8 THE NUMBER OF TRADE AGREEMENTS WITH DATA PROVISIONS IS GROWING



Note: See Annex Table 2 for a list of agreements. The EU is counted as one economy
Source: Own calculations from TAPED database (Burri and Polanco Lazo, 2019).

Trade agreements tend to cover all types of data, but the depth and density of provisions varies from one agreement to another. Some introduce **non-binding guidance** on data flows, including broad provisions affirming the importance of working to maintain cross-border data flows (e.g. the Korea–Peru FTA and Central America–Mexico FTA).[27] Another category of agreements provide language that foresees a **reassessment of data flow provisions in future revisions** (e.g. EU–Japan and EU–Mexico).[28] The last category of trade agreements are those that provide **binding rules on data flows**, relating to transfers of all types of data, often with enforcement mechanisms (e.g. CPTPP and USMCA). The number of trade agreements that fall under the last category has been increasing over the last few years.

27 For instance, Nicaragua-Taiwan FTA Art. 14.05 and Colombia-Costa Rica FTA Art. 16.7 (the original text is in Spanish) stipulate that "[r]ecognizing the global nature of electronic commerce, the Parties affirm the importance of: [...] (c) working to maintain cross-border flows of information as an essential element in fostering a vibrant environment for electronic commerce".

28 For instance, EU-Mexico Modernised Global Agreement Art XX and EU-Japan EPA stipulate that "[t]he Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement".

The agreements that provide rules on data flows and include provisions that foresee unrestricted movement of data also tend to have exceptions allowing parties to restrict the movement of data for legitimate public policy objectives, although they do not usually define what could or could not be regarded as 'legitimate'. Many also enshrine exceptions in the context of both *non-discrimination* and *not unnecessarily trade-restrictive* principles. Furthermore, new agreements, such as RCEP, include a new type of exception that allows parties to apply a measure on data flows to protect "essential security interests". [29]

Increasingly, trade agreements also tackle elements of 'trust'. Indeed, all 29 trade agreements with data flow provisions also include provisions related to the protection of personal information and consumer protection. While some just recognise the importance of such provisions, *all agreements* that include binding data flow rules also require or promote the adoption of domestic privacy and data protection legislation. This includes encouraging parties to take into account international standards and guidelines on protection of personal information (including some detailed under the plurilateral arrangements section).[30]

In sum, the analysis suggests that, in trade agreements, binding data flows provisions go hand-in-hand with exceptions for legitimate public policy objectives and/or provisions on privacy and consumer protection. Governments are increasingly turning to trade agreements for the dual purpose of enabling and safeguarding data flows, implicitly recognising that progress in data flows might only be made via progress in personal data protections, including via references to plurilateral arrangements.

6.4 Other stakeholder and technology drive initiatives

The instruments that fall within this category are different to those discussed in the previous sections. Rather than regulatory instruments, these are tools developed by non-governmental organisations with a view to better handling issues around cross-border data flows in the context of privacy and security protection.

Two broad categories emerge in this area:

- **standards**, referring to standards and principles providing guidance on how organisations might manage cross-border transfers in the context of privacy and security risks; and
- **technology-driven initiatives**, referring to the use of privacy-enhancing technologies (PETs) that enable organisations to meet privacy and digital security objectives when transferring data abroad.

29 RCEP also stipulates that measures to protect essential security interests shall not be disputed by other parties.
30 Some of which (USMCA and Australia–Singapore) specify what these international standards and guidelines are.

This is a fast-developing area, as was the case with the other instruments, and the two approaches may often overlap when a firm applies both an ISO standard and uses PETs. These instruments represent organisational tools that attempt to tackle trusted data flows from a different perspective.

Turning first to **standards**, the International Organization for Standardization (ISO), an independent, non-governmental international standard-setting body composed of representatives from various national standards organisations, has developed standards related to privacy and personal data protection. For example, ISO/IEC 27701:2019[31] specifies requirements and provides guidance for establishing, implementing, maintaining and improving privacy information management systems (PIMS).[32] More specifically, the standard provides guidance for personally identifiable information (PII) controllers and processors and is aimed at helping organisations comply with domestic data regulations, including GDPR. In terms of collection and processing of PII across borders, the standards require organisations to specify and record the countries and international organisations to which data is transferred.[33] Organisations are also called to reject any disclosures that are not legally binding[34] and notify customers of any legally binding requests for disclosure to third parties such as law enforcement agencies. These standards could help companies comply with domestic data governance legislation.

Technology-driven initiatives may also enable greater 'trust' in cross-border data flows. Privacy-enhancing technologies (PETs), such as cryptography are designed to prevent and mitigate the risk of privacy and confidentiality breaches and enable organisations to better manage data responsibly (OECD 2017, 2019, 2020b). In addition, data sandboxes offering strong levels of control and protection of data could also be leveraged towards enabling cross-border access in the case of specific types of data (OECD 2019).

Homomorphic encryption is "a form of encryption that allows certain computations on encrypted data, generating an encrypted result which, when decrypted, matches the result of the same operations performed on the data before encryption". It can be used "to analyse data in circumstances where all or part of the computational environment is not trusted, and sensitive data should not be accessible" (The Royal Society 2019). For instance, homomorphic encryption enables a user to encrypt data, send it to the cloud for processing, and have the output of the computation sent back to be decrypted to obtain the result the user wanted, while maintaining the privacy of the individual and confidentiality of the data. The UK's NHS Digital is using homomorphic encryption to

31 https://www.iso.org/standard/71670.html
32 A 'privacy information management system' refers to an information security management system that addresses the protection of privacy as potentially affected by the processing of personally identifiable information (ISO/IEC 27701:2019, 3.2).
33 ISO/IEC 27701, 7.5.2.
34 ISO/IEC 27701, 8.5.5.

enable safer sharing and linkage of patient-level data between authorised parties, aiming to improve health and care service through research and planning (The Royal Society 2019).[35]

Data sandboxes are isolated environments through which data can be accessed and analysed and where analytic results are only exported, if at all, when they are non-sensitive. These sandboxes can be isolated virtual machines that cannot be connected to an external network and/or machines which require a physical on-site presence at the facilities of the data holder (where the data is located) (OECD 2019). The Centers for Medicare and Medicaid (CMS) Virtual Research Data Center (VRDC) is a virtual research environment that provides timely access to Medicare and Medicaid programme data, such as beneficiary-level protected health information. Researchers working in the CMS VRDC have direct access to approved data files, can conduct their analysis within the CMS secure environment and can download aggregated reports and results to their own personal workstation (OECD 2019).

7 CONCLUDING REMARKS

Understanding how data creates value and how it supports economic activity, and identifying the challenges that data raises, is key to making the most out of the digital transformation. Data is different – it cannot be depleted and can be shared and re-used by many different users and for many different purposes. This means that data sharing has the potential to give rise to considerable economies of scale and scope. However, as more and more data crosses borders, new challenges emerge. These are being met with new data regulation that either conditions the movement of data or mandates that it be stored locally.

The resulting patchwork of rules and regulations is making it difficult not only to enforce privacy and data protection across different jurisdictions, but also for firms to operate across markets, affecting their ability to internationalise and draw benefits from operating on a global scale. Understanding the evolving regulatory environment is an important first step in helping economies meet the dual goal of ensuring that data can flow across borders with trust.

As has been shown, a number of policy approaches and instruments have emerged to enable data to flow across borders while creating trust and mitigating potential risks. However, there is no one, single mechanism to enable data to flow with trust. Countries pursue different, or even multiple and complementary, approaches. Moreover, instruments differ in both their degree of binding and their enforcement mechanisms. For instance,

35 *Pseudonomysation*, defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, is also recognised by GDPR (art. 4 (5)) as an appropriate measure to ensure the privacy of personal data, subject to certain conditions. However, since inclusion in GDPR, research has shown that pseudonomysed data may be easily de-anonymised. Questions are therefore emerging on the efficacy of this type of measure to withstand progress in re-identification methods (OECD 2020a).

many of the plurilateral arrangements, such as the OECD Privacy Guidelines, and about half of the data flow provisions in trade agreements are non-binding. In terms of enforcement mechanisms, domestic regulators play a key role by providing the regulatory infrastructure to enforce issues at the domestic level. However, international enforcement may be more complex.

Although the emerging policy landscape appears to be fragmented, this mapping exercise shows that there are some areas of overlap. A range of **commonalities** between and within instruments emerge. For instance, whether through unilateral mechanisms, trade agreements or plurilateral arrangements, there appears to be consensus on the dual goal of safeguarding data and enabling its flow across borders. Indeed, plurilateral arrangements tend to promote coordination on personal data protection with a view to facilitating cross-border data flows between participating countries. At the same time, domestic frameworks tend to provide unilateral mechanisms to transfer data with safeguards (albeit with differences related to how and by whom the safeguarding is done). Commonalities are also found within instruments, as is the case of contracts or adequacy decisions as unilateral mechanisms foreseen in domestic frameworks (despite differences in whether these are applied ex-ante or ex-post and the extent of government involvement).

There is also growing evidence of **convergence**, often on the basis of the aforementioned commonalities. For instance, trade agreements increasingly include binding provisions on data flows in conjunction with exceptions and requirements for privacy and consumer protection frameworks. At the same time, there is growing evidence of increasing overlaps in the principles that underscore privacy and personal data protection frameworks, including in the context of plurilateral arrangements.

Finally, there exists a degree of **complementarity** between instruments. Unilateral mechanisms draw from, and contribute to, plurilateral arrangements, and trade agreements increasingly reference plurilateral data protection arrangements along with their binding data flow provisions. The emergence of technology approaches to create trusted environments, for example through sandboxes or privacy enhancing technologies, could also help to enable cross-border data flows with trust in the context of unilateral mechanisms, plurilateral arrangements or trade agreements.

The internet is global and borderless, but regulations are not. Ensuring the free flow of data with 'trust' has been a challenge for policymakers for many years. Different solutions to this complex challenge have emerged, albeit mostly in the context of unilateral approaches. International cooperation on these issues, while difficult, can help to reconcile differences. By highlighting commonalities, complementarities and elements of convergence between and within existing approaches, this chapter aims to support continued dialogue in this area to help identify where efforts might be most fruitful. It is

hoped that this will facilitate international cooperation and dialogue on more predictable and transparent combinations of flows and 'trust' that enable governments, firms and consumers to benefit from continued growth, wellbeing and inclusion.

REFERENCES

Acquisty, A, C Taylor and L Wagman (2016), "The Economics of Privacy", *Journal of Economic Literature* 52(2).

Brynjolfsson, E and K McElheran (2019), "Data in Action: Data-Driven Decision Making and Predictive Analytics in U.S. Manufacturing", Rotman School of Management Working Paper No. 3422397 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3422397).

Brynjolfsson, E and K McElheran (2016), "The rapid adoption of data-driven decision-making", *American Economic Review* 106: 133-139 (http://dx.doi.org/10.1257/aer.p20161016).

Burri, M and R Polanco Lazo (2019), "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset", *SSRN Electronic Journal* (http://dx.doi.org/10.2139/ssrn.3482470).

Casalini, F and J López González (2019), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers No. 220 (https://dx.doi.org/10.1787/b2023a47-en).

CISCO (2020), "Cisco Annual Internet Report (2018–2023)", White Paper (www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf).

Economist (2017), "The world's most value resource is no longer oil, but data", 6 May.

Ferracane, F and E Van der Marel (2018), "Do data policy restrictions inhibity trade in services?", European Centre for International Political Economy Working Paper (https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf).

Innovation, Science and Economic Development Canada (2019), *Canada's Digital Charter in Action: A plan by Canadians, for Canadians* (www.ic.gc.ca/eic/site/062.nsf/vwapj/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf).

López González, J and M Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", OECD Trade Policy Papers No. 205 (https://dx.doi.org/10.1787/524c8c83-en).

Mandel, M (2017), *The Economic Impact of data: Why data is not like oil*, Progressive Policy Institute (www.progressivepolicy.org/publications/economic-impact-data-data-not-like-oil).

MGI – McKinsey Gobal Institute (2016), *Digital Globalization: The new era of global flows*, McKinsey & Company (www.mckinsey.com/business-functions/mckinsey-digital/ourinsights/digital-globalization-the-new-era-of-global-flows).

National Board of Trade Sweden (2015), *No Transfer, No Production – a Report on Cross-Border Data Transfers, Global Value Chains and the Production of Goods* (www.kommerskollegium.se/globalassets/publikationer/rapporter/2016-och-aldre/no-transfer-no-production-a-report-on-crossborder-data-2015.pdf)

National Board of Trade Sweden (2014), No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden (www.kommerskollegium.se/globalassets/publikationer/rapporter/2016-och-aldre/no_transfer_no_trade_webb.pdf).

Nguyen, D and M Paczos (2020), "Measuring the Economic Value of Data and Cross-Border", OECD Digital Economy Papers No. 297.

OECD (2020a), *Mapping Approaches to Data and Data Flows*, Report for the G20 Digital Economy Task Force (www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf).

OECD (2020b), "Keeping the Internet Up and Running in Times of Crisis", OECD Policy Responses to Coronavirus (COVID-19) (https://read.oecd-ilibrary.org/view/?ref=130_130768-5vgoglwswy&title=Keeping-the-Internet-up-and-running-in_times-of-crisis).

OECD (2019), "Digital Opportunities for Trade in the Agriculture and Food Sectors", OECD Food, Agriculture and Fisheries Papers No. 122 OECD (https://doi.org/10.1787/91c40e07-en).

OECD (2019), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies (https://doi.org/10.1787/276aaca8-en).

OECD (2017), "Digital risk and trust", in *OECD Digital Economy Outlook 2017* (http://dx.doi.org/10.1787/9789264276284-9-en).

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being* (https://dx.doi.org/10.1787/9789264229358-en).

OECD, WTO and IMF (2020), *Handbook on Measuring Digital Trade* (https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf).

Posner, R (1981), "The Economics of Privacy", *American Economic Review* 71(2): 405-409.

Rowley, J (2007), "The Wisdom Hierarchy: Representations of the DIKW Hierarchy", *Journal of Information Science* 33(2) (http://dx.doi.org/10.1177/0165551506070706).

Solove, S (2006), "A taxonomy of privacy", *University of Pennsylvania Law Review* 154(3): 477.

The Royal Society (2019), *Protecting privacy in practice : the current use, development and limits of privacy enhancing technologies in data analysis* (https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf).

ABOUT THE AUTHORS

Javier López-González is a Senior Trade Economist at the Trade and Agriculture Directorate of the OECD. His recent work focuses on the analysis and measurement of digital trade, including on issues related to cross-border data flows. He has previously also worked on the drivers and implications of participation in global value chains, co-authoring papers on global patterns of supply chain trade; the implications of GVC participation for developing countries; the links between GVC participation and wage inequality; and how SMEs can make the most out of GVC participation. Javier holds a PhD in Economics from the University of Sussex.

Franscesca Casalini is a Policy Analyst in the Trade and Agriculture Directorate of the OECD, where she works on topics related to digital trade, with a focus on cross-border data flows and privacy, and on digital innovation and resilience to natural hazards in the agricultural sector. Francesca holds a Master's degree in International Law from the Graduate Institute of Geneva.

Taku Nemoto is a policy analyst in the Trade and Agriculture Directorate of the OECD, where he works on international trade topics related to digital trade, including cross-border data flows, and industrial subsidies. Taku holds a Juris Doctor degree from the University of Tokyo and a Master's degree from Harvard Law School. He is qualified as a lawyer in Japan.

ANNEX 1 EXAMPLES OF PLURILATERAL ARRANGEMENTS

Non- binding plurilateral agreements	
OECD Privacy Guidelines	**ASEAN PDP Framework**
Australia, Austria, Belgium, Canada, Chile, Colombia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Republic of Korea, Latvia, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States.	Brunei, Cambodia, Indonesia, Lao, Malaysia, Myanmar, Philippines, Singapore, Thailand, Viet Nam.
Binding plurilateral agreements	
Malabo Convention African Union Convention on Cyber Security and Personal Data Protection	**CONVENTION 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)**
The African Union Convention on Cyber Security and Personal Data Protection has not entered into force yet, the following are the ratifying countries as of latest available data published 18/06/2020: Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda, and Senegal.[36]	Albania; Andorra; Armenia; Austria; Azerbaijan; Belgium; Bosnia and Herzegovina; Bulgaria; Croatia; Cyprus; Czech Republic; Denmark; Estonia; Finland; France; Georgia; Germany; Greece; Hungary; Iceland; Ireland; Italy; Latvia; Liechtenstein; Lithuania; Luxembourg; North Macedonia; Malta; Monaco; Montenegro; Norway; Netherlands; Poland; Portugal; Republic of Moldova; the Russian Federation; Slovak Republic; Romania; San Marino; Serbia; Spain; Slovenia; Sweden; Switzerland; Turkey; Ukraine; the United Kingdom; Argentina; Burkina Faso; Cabo Verde; Morocco; Mauritius; Mexico; Senegal; Tunisia; Uruguay.
APEC Privacy Framework	**2013 Additional Protocol to the Convention**
Australia; Brunei Darussalam; Canada; Chile; China; Hong Kong, China; Indonesia; Japan; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Philippines; the Russian Federation; Singapore; Republic of Korea; Chinese Taipei; Thailand; Viet Nam; and the United States.	Albania; Andorra; Armenia; Austria; Belgium; Bosnia and Herzegovina; Bulgaria; Croatia; Cyprus; Czech Republic; Denmark; Estonia; Finland; France; Georgia; Germany; Hungary; Ireland; Latvia; Liechtenstein; Lithuania; Luxembourg; North Macedonia; Monaco; Montenegro; Netherlands; Poland; Portugal; Republic of Moldova; the Russian Federation; Slovak Republic; Romania; Serbia; Spain; Sweden; Switzerland; Turkey; Ukraine; Argentina; Cabo Verde; Morocco; Mauritius; Senegal; Tunisia; Uruguay
APEC Cross-Border Privacy Rules (CBPR) System	**2018 Protocol amending the Convention**
The United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, the Philippines; and Chinese Taipei. With more expected to join soon	Bulgaria, Croatia, Cyprus, Estonia, Lithuania, Poland, Serbia, Mauritius

Note: OECD economies in bold. Data valid as of 02/11/2020.

36 According to the most recent accessible official document online.

ANNEX 2 TRADE AGREEMENTS WITH DATA PROVISIONS.

Agreement
CPTPP (Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam)[1]
USMCA (Canada, Mexico and the United States)
Korea-US FTA
Chinese Taipei - Nicaragua FTA
Canada - Peru FTA
Caribbean Forum - EC EPA
Cameroon - EC Interim EPA
Hong Kong - New Zealand FTA
Korea - Peru FTA
Central America – Mexico FTA
Colombia - Costa Rica FTA
Canada - Honduras FTA
Pacific Alliance Additional Protocol (PAAP)
Mexico - Panama FTA
Canada - Korea FTA
Japan - Mongolia FTA
Korea - Vietnam FTA
Chile - Uruguay FTA
Australia – Singapore FTA
Argentina - Chile FTA
Singapore – Sri Lanka FTA
Australia - Peru FTA
EU - Mexico Modernised Global Agreement
Brazil - Chile FTA
EU - Japan EPA
Indonesia - Australia CEPA
Japan - US Digital Trade Agreement
Digital Economy Partnership Agreement between Chile, New Zealand and Singapore (DEPA)
Singapore - Australia Digital Economy Agreement (SADEA)

Source: Own calculations from the TAPED database.

CHAPTER 3

An AI policy for the (near) future

Bryan Mercurio and Ron Yu
The Chinese University of Hong Kong

1 THE AMBIT OF THIS CHAPTER

Artificial intelligence (AI) is one of the big technological disruptions that will require a governance framework, including on access to data as part of AI technologies. This chapter seeks to uncover new insights on how policy could tackle existing or future impediments and how trade agreements can be used to enhance the United Kingdom's position in digital trade and data governance, and to identify important considerations for negotiations of free trade agreement (FTAs).

Assessing trade-related and intellectual property (IP)-related AI issues is complicated by the fact that AI systems may enjoy a high degree of autonomy and movement and can train themselves and adapt to the environment without human intervention. (Barfield 2018, WIPO 2021). Further complicating the assessment is the fact that the development and use of AI builds on other digital technologies – notably, cloud computing, big data, and the Internet of Things – that also rely on cross-border data flows, thereby potentially drawing in matters of cybersecurity, ethics, privacy, competition, trade secrets as well as enforcement, justice and equity, taxation and displacement of labour (Calo 2018).

To avoid becoming too unwieldy, this chapter focuses primarily on trade and non-trade secret IP and data matters, considering policy priorities that include the promotion of the development of local expertise, protection of indigeneous IPR, innovation and industry, trade and safety. The emphasis will be on the substantive issues of AI and its implications for IP and data-related matters, with a specific focus on how to embed the policy choices in trade agreements.

The chapter will not cover issues of bias in AI[1] and AI ethics, taxation, geopolitical considerations and privacy (except where it impacts AI system training, data flows and trade). Other issues beyond the scope of the chapter include liability issues related to AI (for example, badly designed or implemented AI systems), employment and regulatory matters. Examples here include the use of AI in cross-border tele-diagnosis, the role of AI in distinguishing trademarks or to influence consumer behaviour and issues involving cybersecurity, trade secrets, the impact on jobs, privacy, the use of AI during

1 Many AI technologies are based on data, rules and other inputs from human experts. As all humans are intrinsically biased to some degree in one way or another, so is the AI.

the examination and prosecution of IPRs, expedited prosecution of AI-related patents and the use of AI to track misuse and enforce IP protection. Issues such as using AI in scrutinising trade (for example, to examine imported items) and how AI could be unintentionally (or deliberately) erecting roadblocks to trade are also not discussed in this chapter. Finally, despite the fact that AI has the potential to improve outcomes in international trade negotiations (for instance, it could be used to better analyse economic trajectories of each negotiating partner under different assumptions), developments in this area will not be discussed (UNCTAD 2018).

2 INTRODUCTION

AI will bring both advances and challenges to governments and industry. Advances in AI technologies are pushing the frontier of what machines are capable of doing and have already diffused into many businesses and sectors. AI has the potential to transform operations and business models, eventually powering higher productivity and growth across economies. One of the four Grand Challenges forming the UK Government's Industrial Strategy, the development of 'AI and data' is recognised as a potential driver of growth (UK Department of Business, Energy and Industrial Strategy 2021) In fact, the UK IP Office estimated that AI will add £630 billion to the UK economy by 2035 (UK Intellectual Property Office 2019), while McKinsey projects that by 2030 AI could uplift the global economy by as much as 16% and boost the UK economy by as much as 22% (McKinsey Global Institute 2019) As more economies incorporate and make more effective use of AI, the technology's impact will continue to grow (Brynjolfsson et al. 2017).

AI will also impact the type and quality of economic growth (with implications for international trade patterns and relationships), accelerate the transition towards a services economy, and significantly alter the development and management of global value chains.[2] Even now, millions of creators across the globe earn money on AI-powered platforms. AI-developed translation services are further enabling digital platforms as drivers of international trade, and should AI increase productivity, then economic growth and new opportunities for international trade will likewise increase (Brynjolfsson et al. 2017, Meltzer 2018, Klein 2020). Not all the by-products of AI will be positive, however, with jobs at home and abroad at risk (Arntz et al. 2016).

Despite a growing literature exploring AI's challenges in both international law and global governance, far less attention has been devoted to this matter from the standpoint of international trade and IP law. For example, the European Commission's "Ethics Guidelines for Trustworthy AI" failed to reference how cross-border trade bears on the

2 For example, AI can help businesses improve predictions of future trends, better manage risk along the supply chain and better manage complex and dispersed production units to, inter alia, improve warehouse management, demand prediction, and improve the accuracy of just-in-time manufacturing and delivery, increase productivity and efficiency in packing and inventory inspection, improve physical inspection and maintenance of assets along supply chains.

EU's normative approach to AI or the more complex trade issues raised by AI. With regards to trade, the white paper on AI (European Commission 2020a) only notes:

> The EU will continue to cooperate with like-minded countries, but also with global players, on AI, based on an approach based on EU rules and values (e.g. supporting upward regulatory convergence, accessing key resources including data, creating a level playing field) The Commission will closely monitor the policies of third countries that limit data flows and will address undue restrictions in bilateral trade negotiations and through action in the context of the World Trade Organization.

Such an oversight can result in serious policy blind spots, given the aforementioned importance of cross-border data flows and that AI systems often do not easily fall within the categories set forth by the two major agreements that underpin the World Trade Organization (WTO) – the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS) – not only because these agreements were negotiated prior to AI's existence, but also because they are largely agnostic as to the medium through which trade is conducted (Yu 2014). This problem of classification can be illustrated by taking an AI tool and attempting to classify it under the GATS and GATT as its functional capabilities increase. In this regard, Liu and Lin (2020) cite ROSS Intelligence, an AI-powered program that uses natural language processing to help conduct legal research and document reviews on American laws and several potential problems, such as:

- If ROSS (or its equivalents) evolved to generate well-structured, human-like responses such as a lawyer providing legal services, could a WTO Member ban ROSS's website since ROSS is not technically a lawyer?
- What would be the issues if a state bar association/jurisdiction formally recognised AI lawyers or granted them legal personality?
- If an advanced ROSS is embodied in a physical form, could it even be governed by GATS or GATT?

The UK's challenge is to harness the benefits of AI while at the same time guarding and mitigating against foreseeable risks. The UK has the greatest density of AI start-ups launched in the areas of health and medical technology in Europe (Drayson 2019), and several leading AI firms, including DeepMind (acquired by Google), SwiftKey (acquired by Microsoft), VocalIQ (acquired by Apple) and Magic Pony (acquired by Twitter), were all started in the UK. That being said, most successful British AI firms are eventually acquired by larger foreign companies and the UK pales in comparison to the United States and China as the world's powers in the development and deployment of AI (McKinsey Global Institute 2019). This is a reality which is unlikely to change in the foreseeable future.

It is also important to understand that there is a difference between discoveries and implementation – the US is the world's leader in AI discoveries, while China is the leader in AI implementation (Lee 2018) – and that development of the UK's AI capacity will not only depend on domestic but also international matters. While AI often interacts with cyberspace and shares some similarities with the internet, its unique features pose new challenges that many trade lawyers have never seen and that already flummox IP professionals.

3 FINDING COMMON GROUND

In formulating innovation, IP and trade policies, a common definition of AI and AI-related terms is necessary. This is a point UK Under Secretary of State at the Department for Business, Energy and Industrial Strategy, Amanda Solloway, stressed during the November 2020 World Intellectual Property Organization (WIPO) Conversation on AI. Such a definition would demonstrate consistency and lead to confidence, which could aid in unlocking the vast global investment needed to bring AI technologies to market by providing the predictability business, investors, and researchers need to operate (WIPO 2021). The definition would also assist the government and its trade negotiators in ensuring treaty texts match governmental priorities, aims and objectives.

The problem at this time is that the complicated and evolving nature of AI has led to international definitional inconsistency. While the UK's House of Lords referred to AI as technologies with the ability to "perform tasks that would otherwise require human intelligence such as visual perception, speech recognition, and language translation" (House of Lords 2019), on its website the UK Office for Artificial Intelligence (2019) defines AI in the following terms:

> ...a research field spanning philosophy, logic, statistics, computer science, mathematics, neuroscience, linguistics, cognitive psychology and economics... AI can be defined as the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence...AI is constantly evolving, but generally it involves machines using statistics to find patterns in large amounts of data, is the ability to perform repetitive tasks with data without the need for constant human guidance...
>
> Machine learning is the most widely used form of AI, ... Machine learning can be:
>
> - supervised learning which allows an AI model to learn from labelled training data;
> - unsupervised learning which is training an AI algorithm to use unlabelled and unclassified information;
> - reinforcement learning which allows an AI model to learn as it performs a task.

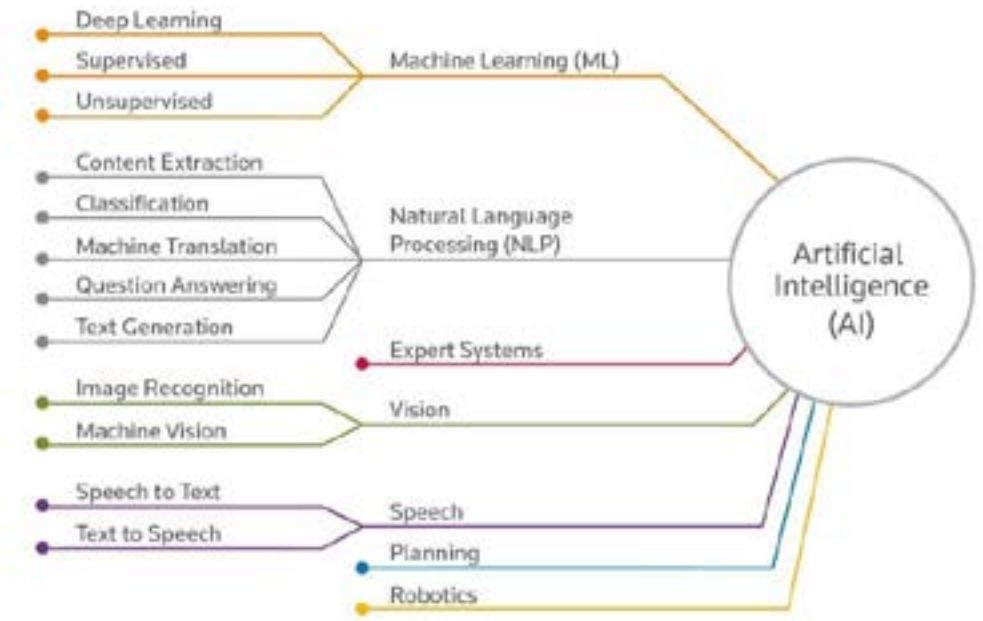
Other jurisdictions provide differing definitions of AI, as the following examples illustrate:

- Singapore refers to AI as "a set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning, and, depending on the AI model, produce an output or decision (such as a prediction, recommendation, and/or classification). AI technologies rely on AI algorithms to generate models. The most appropriate model(s) is/are selected and deployed in a production system" (Singapore PDPC 2020).
- Australia refers to AI as "a collection of interrelated technologies used to solve problems autonomously, and perform tasks to achieve defined objectives, without explicit guidance from a human being" (Australia Department of Industry, Science, Energy and Resources 2020).
- Taiwan defines AI as "systems acting as humans [and] systems acting rationally" (Liu and Lin 2020, citing Taiwan's Basic Act for Developments of Artificial Intelligence).
- The European Commission's High-Level Expert Group on AI concludes that "AI gives machines the capability to analyse their environment and take decisions with some degree of autonomy to achieve specific goals…Machine learning (ML) denotes the ability of software and computers to learn from their environments or from very large sets of representative data. This enables systems to adapt their behaviour to changing circumstances or to perform tasks for which they have not been explicitly programmed" (European Commission 2021).

Other nations do not offer a clear-cut definition of AI. For example, China's 2017 New Generation of Artificial Intelligence Development Plan mentions but does not actually define AI (China State Council 2017).

To further complicate matters, AI is an evolving constellation of technologies (Chessen 2017) – an umbrella term that encompasses computer engineering techniques, with the main streams being machine learning, natural language processing, expert systems, vision, speech, planning and robotics (Kemp 2020). Figure 1 illustrates the progression of streams and constellations that go into AI.

FIGURE 1 THE MAIN AI STREAMS



Source: Kemp IT Law (www.kempitlaw.com/wp-content/uploads/2020/06/Algo-IP-Main-AI-streams-Blog-4.jpg).

A final point to understand is that there are key differences between narrow (weak) AI, which is capable of carrying out specific tasks (such as translation services, chatbots, autonomous vehicles), and generalised AI, which "exhibits apparently intelligent behaviour at least as advanced as a person across the full range of cognitive tasks" and is essentially "intellectually indistinguishable from a human being" (National Science and Technology Council Committee on Technology 2016). Generalised AI requires capabilities that go beyond today's approach in ML. Moreover, developments in AI are increasingly focused on developing more thoughtful approaches to analysis, in what Daniel Kahneman has labeled System 2 thinking (he describes System 2 thinkers as slower, more deliberative, and more logical than the faster, more impulsive System 1 types) (Kahneman 2011, MBZUAI 2020).

Problems may arise when AI-related terms are applied interchangeably not just due to technological differences but also to the implications associated with the different AI technologies. For example, ML requires a well thought-out training and data acquisition strategy and has the capacity to improve its performance in a task over time, unlike, for instance, rules-based systems and generalised AI, which will likely require additional technological breakthroughs to be realised (Surden 2014, Marcus 2018).

The difficulty for the UK will be in capturing the concept of AI and formulating a technologically neutral, future-proof framework for AI, given the rapidly evolving field and technologies and the fact that global definitions are likely to remain diverse and

unharmonised. That being said, the UK should set out a basic definition of AI and AI-related terms for internal use in order to facilitate policy formulation amongst different departments and a wide range of stakeholders and impacts on society (e.g. ethics, innovation, IP, taxation, commerce and trade). In so doing, policymakers need to keep in mind that an overly broad definition may be insufficient when it comes to precisely defining the particular AI subject matter for which specific protections are sought, as different AI technologies and aspects may raise distinct issues.

4 INTELLECTUAL PROPERTY

The question of AI and IP is both contemporary and pressing, and prompted WIPO to hold multiple "Conversation on IP and AI" events in September 2019, followed by a public consultation in which it received over 250 submissions, a consultation paper, an event in February 2020 on "Copyright in the Age of Artificial Intelligence", and second and third conferences in July and November 2020 (WIPO 2020a, WIPO 2020b).

AI-related IP issues are far more complicated and involved than they might initially appear, given the speed at which advances in AI technology occur, giving rise to the need to improve IP policies and guidelines. Policymakers need to take cognizance of the fast-changing IP ecosystem and its implications for and impact on people, systems and society, as well as the fact that current laws never envisaged a situation where AI systems could create and invent on their own, with a minimal nexus with a human being. In such a circumstance, listing the human as 'author' or 'inventor' may not be feasible or appropriate.

The WIPO efforts are currently focusing on questions related to:

- Do AI-generated content, inventions and the like warrant IP protection? And if AI inventions and creations are allowed IP protection, should there be new systems of examination (for patents) or protection (for copyright) for such works?
- Would the lack of IP protection for AI-generated content and inventions be problematic and would organisations or individuals be incentivised to conceal the involvement of AI if AI inventions and creations are denied IP protection?

Additional difficult legal issues plus a convergence of technical, legal, data-related, social and societal issues must also be studied and addressed. These include:

- challenges to some of the basic terms in IPRs (such as 'inventor', 'owner', and 'author'), the duration of protection, and consideration of new ways to create, enforce and safeguard IP;
- AI-generated deep fakes;
- protection of algorithms;

- sharing of IP;
- issues regarding the use of AI in processing IP applications or expediting the granting of AI-related IPRs; and
- issues regarding the use of AI to limit the choice of trademarked goods or influences on consumers.

AI also raises IP issues with international trade implications, which are primarily data-related and as such will be discussed in the section on data. This section will now, however, address several of the above issues in greater detail.

4.1 Challenges to notions of inventor, owner and author in the age of AI

The replacement of humans in industries that require creativity, curiosity and critical thinking challenge our understanding of 'authorship' (in relation to copyright), 'inventorship' (in terms of patents) of non-human-generated outputs (Davies 2011) and ownership, which is becoming harder to ascertain for outputs generated by advanced AI systems. Such issues are becoming increasingly important, however, as more AI-generated content is released, such as the next-generation robot-journalists (e.g. Toutiao's Xiaomingbot, Forbes's Bertie, Bloomberg's Cyborg and Tencent's Dreamwriter), and as the ability of AI systems to invent on their own grows. To date, most jurisdictions have relied on principles built through jurisprudence to reject the granting of patents or copyright protection to AI 'inventors' and AI-generated content. There are exceptions, however, with China perhaps somewhat surprisingly being one jurisdiction that has granted copyright protection to AI-generated content.

With regards to copyright and AI-generated content, Section 9(1) of the UK Copyright Designs and Patents Act 1988 (CDPA) provides that the author of software (as a literary work) is the person who creates it and that the author is the work's first owner (unless it was created by an employee in the course of his employment, in which case the employer is the first owner). Section 9(3) of the CDPA grants copyright to "the person by whom the necessary arrangements are undertaken" for computer-generated work, which Section 178 defines as a work "generated by computer in circumstances such that there is no human author of the work".[3] There is no significant UK case law interpreting or clarifying the meaning of undertaking "necessary arrangements" for the creation of the work where "there is no human author" (Kemp 2020).

The UK approach is echoed in smaller common law jurisdictions such as New Zealand, Hong Kong and Ireland, but others, including the US, Australia and most civil law countries, take a different stance. For instance, the US Copyright Office applies a "human

3 Sec. 9(3) of the CDPA states: "In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken."

authorship policy" with explicit human authorship requirements and will not register works produced by nature, animals or plants (US Copyright Office 2021). This is in line with US case law, most notably the iconic *Naruto v. Slater*,[4] where the US Ninth Circuit court affirmed the district court's dismissal of copyright infringement claims brought by the People for the Ethical Treatment of Animals (PETA) as a friend to Naruto, a crested black macaque, alleging copyright infringement over selfies he took on a wildlife photographer's unattended camera. Australia takes a similar approach, with the court in *Telstra Corporation Limited v. Phone Directories Company Pty Ltd*[5] underscoring the need for a human author and "some independent intellectual efforts" in order for the granting of copyright. Likewise, in the EU, Article 2(1) of the Directive on the Legal Protection of Computer Programs and Article 4(1) of the Database Directive defines the author as a natural person or group of natural persons who create it, while permitting national laws of a member to otherwise designate the legal person as the right holder.

Somewhat surprisingly, China may also be heading towards a more permissive protection regime for AI. In January 2020, in *Shenzhen Tencent v. Shanghai Yinxun*, a court in Shenzhen awarded RMB1,500 in damages to Tencent for infringement of a financial article written by its robot Dreamwriter without authorisation, on the basis the article possessed some "originality".[6] The court highlighted the detailed inputs of the plaintiff's creative team and concluded that if the software was the subject of creation, it would disregard the personalised arrangement and selection of the creative team. Accordingly, the court declared the plaintiff to be the author, based on an interpretation of Article 11 of the Copyright Law of the People's Republic of China, which grants authorship to the entity under whose supervision and direction the work is created.

Turning to patents and AI-generated inventions, the issue of obtaining patent protection for an AI-generated invention appears at first glance to be straightforward – such an invention would be patentable if it meets the definition as set out by Article 27.1 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which provides:

> ...patents shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application ... and patent rights enjoyable without discrimination as to the place of invention, the field of technology and whether products are imported or locally produced.

Under UK law, an inventor has the right to be mentioned, but the Intellectual Property Office has determined that the naming of a machine as inventor did not meet the requirement in the Patents Act 1977 that a natural person be identified as the inventor. Thus, the IP Office rejected patent applications naming DABUS as the inventor of a "food

4 *Naruto v. Slater*, No. 16-15469, 9th Cir. 2018.
5 *Telstra Corporation Limited v. Phone Directories Company Pty Ltd* [2010] FCAFC 149 (Austl.).
6 Case No. (2019) Yue 0305 Min Chu No. 14010.

container" and a "device and method for attracting enhanced attention" autonomously without any form of human intervention,[7] a decision upheld in *Thaler v The Comptroller-General of Patents, Designs and Trade Marks*.[8] The Intellectual Property Office has subsequently updated its examination guidelines by adding sections 7.11.1 and 13.10.1 to its Manual of Patent Practice to reflect the UK High Court's decision (Hervey 20201). This is in line with decisions of the European Patent Office (EPO) and US Patent and Trademark Office (USPTO), which also denied applications for patents naming DABUS as the inventor.

Potential complications

Thus far, the consensus is that human involvement is a necessary factor for the granting of copyright and patent protection, although in the case of copyright there is disagreement on the required degree of involvement and ownership, and it is from here that problems could potentially arise. The TRIPS Agreement is largely silent on the matter as it merely provides a minimum standard of protection for IPRs (as seen above in regard to Article 27.1), leaving WTO members with wide scope to determine how to appropriately implement the provisions. Should the treatment of AI and AI-generated or AI-assisted content diverge further, this bifurcation within WTO members could become problematic.

Under the TRIPS Agreement, Article 3 imposes national treatment obligations regarding IPRs and protections that include "matters affecting the availability, acquisition, scope, maintenance and enforcement of intellectual property rights as well as those matters affecting the use of intellectual property rights specifically addressed [in the Agreement]". As such, the UK is obligated to grant copyright protection of AI-generated creations to nationals of other WTO members under the standards it sets under the CDPA, but without guarantees of reciprocal protection given that other countries may apply different standards.

Article 9 of the TRIPS Agreement deals with copyright protection but does not define the scope of copyrightable subject matter. Instead, the provision simply refers to the relevant provisions of the Berne Convention including Article 2(1), which defines "protected works" as including, among others, "literary and artistic work", which comprises "every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression" and contains a non-exhaustive list of such works. While Article 2(1) of the Berne Convention does not offer much insight on authorship and the originality requirement, Articles 5(2) and 14bis(2)(a) indicate that the determination of the author of a work and originality is a matter of the law of the country where protection is claimed.

7 BL O/741/19.

8 *Thaler v The Comptroller-General of Patents, Designs and Trade Marks* [2020] EWHC 2412 (Pat)

To add further complexity, even among countries that adopt the UK model, there may be variations in how to interpret the "necessary arrangements" in allocating the authorship. For example, while Commonwealth countries adopting the UK model may accept relevant UK case law as persuasive authority, a civil law country adopting the UK standard may not.

Another potential complication is the scope of allowable exceptions to copyright protection. Whereas the US provides for wide exceptions under its concept of "fair use", the UK and most others allow for narrower and more defined exceptions under "fair dealing" (DACS 2018).

Perhaps for these reasons, governments have been hesitant in addressing copyright standards and flexibilities in trade agreements. For instance, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) merely includes a recognition by the Parties of the need to achieve "an appropriate balance in its copyright and related rights systems."[9] An equivalent clause, however, is absent from the intellectual property chapter of the more recent United States–Mexico–Canada Agreement (USMCA) (Meltzer 2018, Hart 2018).

Finally, as AI allows a large volume of works to be produced in a short space of time, the granting of copyright protection for AI-assisted outputs raises important policy questions, such as the risk of reducing the public domain as a result and whether automated over-production of literary and artistic work may negatively affect the demand for human creation (WIPO 2021).

Term and duration

Questions involving the term of protection and liability are primarily copyright related. Copyright laws provide specific periods of time during which the work and the rights arising thereof are legally protected that are usually determined in reference to the life of work's author (and exceptionally the work's first publication or transmission). The life of the author cannot be used when AI is the author given the theoretically indefinite lifespan of the system, but consensus has not yet emerged on the appropriate length of protection (Gurkaynak et al. 2018).

This issue could arise in a cross-border negotiation where the duration of protection of one jurisdiction is shorter than the equivalent copyright protection applied in the UK.

9 Article 18.66 CPTPP states: "Each Party shall endeavour to achieve an appropriate balance in its copyright and related rights system, among other things by means of limitations or exceptions that are consistent with Article 18.65 (Limitations and Exceptions), including those for the digital environment, giving due consideration to legitimate purposes such as, but not limited to: criticism; comment; news reporting; teaching, scholarship, research, and other similar purposes; and facilitating access works for persons who are blind, visually impaired or otherwise print disabled."

4.2 Algorithms

AI is a combination of software and data[10] but two things distinguish an AI algorithm from traditional software:

- the fact that AI can train itself and adapt to the environment without human intervention and, as a consequence, the relevant AI algorithm's rules and software implementation are themselves dynamic and change as the machine learns, which sometimes results in unpredictable behaviour (Schwartz 2020); and
- the very large datasets that AI algorithms process.

While it is clear that algorithms have value (Heckman et al. 2015, Higgins 2020), the protection of algorithms and algorithmic models used by AI is at present uncertain and difficult to obtain in most jurisdictions.

For instance, Article 9.2 of the TRIPS Agreement notes that copyright protects expressions and not ideas, procedures, methods of operation or mathematical concepts as such. In this regard, it is clear that in the context of software, expressions are protected but the underlying ideas in the software or computer programs – i.e. the AI algorithms and other processes – are not eligible for copyright protection.

With regards to patents, algorithms are not patentable per se – for instance, Sec. 1(2)(c) Patents Act 1977 excludes "a program for a computer" from patent protection to the extent that the patent application "relates to that thing as such". That being the case, current patent laws broadly treat AI inventions as logical algorithms implemented on the computer. In other words, while the AI algorithms might not be patentable themselves, the implementation of the algorithms could be patentable.

The patentability of computer programs is not harmonised across jurisdictions, therefore what may represent patentable subject matter in one country may be excluded from patentability in others. However, all jurisdictions seem to agree that computer programs have to display a direct, technical effect in the real world to be patentable. For example, the use of a neural network and deep learning algorithm incorporated into a physical device monitoring and identifying irregular heartbeats may be eligible for patent protection.

Perhaps owing to the uncertainty of protection under the domestic IP framework, some recent trade agreements (including the USMCA, US–Japan Digital Trade Agreement and UK–Japan Comprehensive Economic Partnership) specifically require protections for algorithms.

10 The data consists of (i) the input training, testing and operational datasets; (ii) the input data as processed by the computer; (iii) the output data from those processing operations; and (iv) insights and data derived from the output data.

5 DATA AND AI

The importance of data to modern AI cannot be overstated. Data, for example to train AI, raises IP and trade, as well as privacy and cybersecurity matters. This chapter will henceforth concentrate on the former two issues.

5.1 The importance of data quantity

Data is vital for training AI; the more data one has, the better. Without access to data, it would be hard to make AI tools that work (MIT Laboratory for Information and Decision Systems 2020). The world leaders in AI achieved their pre-eminence in large part due to access to huge sets of data; the US and China, with large internal populations, are less reliant on access to data from third countries to develop AI capabilities tailored to their domestic markets than the UK. For the UK to develop AI in health care, for example, it would require access to global health data and limits on access to such data would reduce the accuracy and relevance of its AI systems.

5.2 Product development and access

Building AI systems, particularly ones that can respond to diverse challenges and different population groups requires access to global data. To take relatively straightforward examples, the development of speech-recognition AI requires access to large amounts of speech data that can capture local slang and intonation as well as less commonly used words. This can sometimes go astray, as Volvo realised in testing its autonomous vehicles when it discovered the Scandinavian-developed systems could not properly react to the presence of kangaroos in Australia since they had not been trained to deal with the Australian marsupials (Sergeev 2016).

Developers will not only need access to data, but also infrastructure and tools such as Facebook's PyTorch, Google's Tensorflow, Salesforce's Einstein or other cloud-based tools.

5.3 Deployment

Data-related issues are the main reasons for the failure of AI projects (Gonfalonieri 2019). To illustrate this, a survey conducted in 2017 found that 80% of businesses employing AI reported that training their algorithms proved more challenging than expected due to, inter alia, bias or errors in the data, lack of data, data in unusable forms, or lack of people or tools to label data (Ransbotham et al. 2017).

5.4 Policies and implications

Unsurprisingly, government AI policies identify access to data as key for a competitive AI landscape. For example, the EU's AI policy covers measures on the free flow of personal data and non-personal data in the digital single market, the re-use of public sector

information as well as open access for scientific information, among others, with the aim of facilitating data sharing for re-use in the public and in the private sectors (European Commission 2018a).

To build large-scale datasets, UK AI developers can purchase data, generate the data themselves or use low-friction alternatives such as the public domain – though this last option has risks of bias (Calo 2018). Given the size of the UK population, it will not be able to achieve the data scales of larger countries such as the US, China or India by using its local data sources. This limitation will be further exacerbated by the increasing scarcity of large training datasets, not to mention the growing awareness of the business and ethical constraints of problems of data-hungry systems – i.e. that not all organisations have the volume of data necessary to build unique capabilities using neural networks, and that using huge amounts of peoples' data raises privacy issues or the fear of litigation because it is not clear how such systems use input data to arrive at bad unexplainable outcomes (Wilson et al. 2019). Therefore, building the large datasets will likely require some form of data-sharing with other nations.

Alternatively or in parallel, the UK can investigate technology to build AI that is less reliant on large datasets – for example, one-shot learning or dataset distillation – or looking at generating data using computer programs to train AI systems such as synthetic data (Xu et al. 2019, Sucholutsky and Schonlau 2020a, 2020b). These technologies, of course, will have significant IP attached – for instance, in the case of synthetic data to not only the data but also data curation and data model aspects.

5.5 Intellectual property issues related to data

As noted earlier, data is a crucial element of AI and AI relies on large amounts of input data. Training data will often need to be copied and edited for use. Depending on how the data is collected, this could involve unauthorised copying of thousands of protected works.

Both the Berne Convention and the TRIPS Agreement provide for exceptions to copyright infringement depending on the purposes of the use of an otherwise protected work. For instance, Article 9(2) of the Berne Convention establishes three conditions for exceptions and limitations to the right of reproduction: (i) only in certain special cases; (ii) only if there is no conflict with a normal exploitation of works; and (iii) only if there is no unreasonable prejudice to the legitimate interests of authors. Article 13 of the TRIPS Agreement provides similar criteria.

In the UK, exemptions are provided under a fair dealing regime. Similarly, Article 3 of the 2019 European Union Directive on Copyright and Related Rights in the Digital Single Market provides an exception for text and data mining for scientific research. Such an approach can offer specific assurances about the types of AI uses of copyrighted works that are not infringements but does not take steps to facilitate compensated uses of copyrighted training data; text and data mining exceptions are being discussed or have been implemented in many jurisdictions (Sobel 2017).

This contrasts with the fair use doctrine of the US, which provides for a more flexible principles-based set of copyright exceptions. The fair use doctrine allowed for a significant legal underpinning in the development of digital business models in the US, particularly as American courts have held that the use of large volumes of copyrighted literary work for machine mining fell within the fair use exception. Such decisions have been primarily based on the fact that the data use did not provide an alternative version of the copyrighted literary work to the public, but instead only used snippets of it.[11]

The extent of domestic exceptions to copyright are the result of deliberate policy choices, and therefore reconciling fair use and fair dealing will simply not occur in an international trade agreement (nor should it). Even limited progress – for instance, on the definition of 'fair' in fair dealing or standards in the application of the four-factor test of fairness in fair use (purpose and character of the use, nature of the work, amount used and the substantiality of what has been taken from the work and effect of the use on the potential market value for the work) – will be difficult to achieve.

In this regard, speakers at the November 2020 WIPO Conversation on IP and AI were in general agreement on the need to balance the desire of AI developers to access large volumes of data and the rights of copyright owners in protected works included in the data, but they were divided on possible solutions. Some opined that data mining provisions or the fair use doctrine would provide adequate exceptions to copyright, others warned against harming the rights and interests of creators, while others suggested that broad access and use of copyrighted works should be allowed to help reduce bias and that fear of liability for copyright infringement might also prevent AI researchers from releasing the data on which the AI was trained, reducing AI explicability and transparency.

The debate on the protection of data is complicated by a need to consider the many different types and sources of data and what constitutes infringement in the new AI age – i.e. whether using copyrighted works to train AI could be considered non-infringing by default since such uses do not compete with the original works in any market.

Some points for consideration:

- Do current mechanisms, such as contacts, licenses and trade secrets, provide adequate data protection?
- Would the introduction of new rights for data in the UK risk impeding or disincentivising innovation by creating unnecessary barriers?

11 See, for example, *Authors Guild v. HathiTrust*, 755 F.3d 87 (2d Cir. 2014), *White v. West* (S.D.N.Y. 2014); *Fox v. TVEyes* (S.D.N.Y. 2014); *Authors Guild v. Google*, 770 F.Supp.2d 666 (S.D.N.Y. 2011); *A.V. v. iParadigms*, LLC (4thCir. 2009); *Perfect 10 v. Amazon*, 508 F.3d 1146 (9thCir. 2007); *Field v. Google*, 412 F.Supp.2d 1106 (D. Nv. 2006); and *Kelly v. Arriba Soft*, 336 F.3d 811 (9thCir. 2003).

- Should certain types of data (such as earth remote sensing data) which represent a significant investment to produce be classified as an asset? If so, ownership would need to be established and it is doubtful that existing IPRs would be capable of effectively protecting the data or resulting products or safeguarding the sizable investments needed to create the infrastructure required to collect and process those data.
- Should there be a right to access non-personal data to facilitate access to data or a right of access to non-personal data, for example, in the context of interoperability between interconnected devices and data portability?

5.6 Protecting data

Although a finalised AI product may give the impression that it is able to learn on its own, in the background experienced human data scientists are still needed to frame the problem, prepare the data, determine appropriate datasets, remove potential bias in the training data and, most importantly, continually update the software to enable the integration of new knowledge and data into the next learning cycle (Hippold 2020). While many focus on data volumes, data-related issues are often overlooked, which is unfortunate given that the effectiveness of an AI is not a function of the algorithm alone but of the algorithm after it has been trained on some dataset. (Wei 2020) Thus it is perhaps unfortunate that IP protections for data, database and data curation issues are limited.

Databases

Under Sec. 3A(1) of the CDPA, a "database" is essentially a collection of independent works, data or other materials that are arranged in a systematic or methodical way and are individually accessible by electronic or other means. The first owner of the database is its maker, with the database "maker" being defined in Reg. 14(1) and 15 as "the person who takes the initiative … and assumes the risk of investing" in its contents.

Unlike copyright, the rules on ownership of database rights do not envisage computer-generated databases. The ownership position nevertheless raises a host of important questions and considerations. For instance, would the maker of a database using data generated by sensors or other technology be the manufacturer of the sensor/technology rather than the entity deploying or using the sensor/technology for specific purposes (Kemp 2020)?

In building a database, considerable resources may be spent finding suitable training data, correcting training errors, or ensuring the data has not been corrupted (for example, by a cyberattack). Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases grants copyright protection to databases which, as such, by reason of the selection or arrangement of their contents, constitute the "author's own intellectual creation" and offers additional *sui generis* protection to reward the substantial investment of the database maker in creating the database and prevent free-riding on somebody else's investment in creating the database, existing in parallel

with the copyright protection on the structure of the database (Debusshe and Cesar 2019). However, with regard to copyright and *sui generis* database rights arising as from 1 January 2021, *sui generis* database rights in the EU are not valid in the UK (and vice versa). EU residents and entities are excluded from *sui generis* database rights protection in the UK and UK residents and entities are excluded in the EU (UK Intellectual Property Office and Government Digital Service 2020).

In comparison, the US protects databases to some extent under copyright law as compilations – defined in 17. U.S.C. § 101 as a "collection and assembling of pre-existing materials or of data that are selected in such a way that the resulting work as a whole constitutes an original work of authorship". Such protection is of limited value, however, as the US Supreme Court in *Feist Publications, Inc. v. Rural Telephone Service Co.*[12] held that a compilation of facts is copyrightable only if the selection or arrangement "possesses at least some minimal degree of creativity." Pre-existing materials or data included in the database therefore may be protected by copyright or may be unprotectable facts or ideas.

Some laws, such as those in the Nordic countries, contain some features not found in other laws. For example, under Swedish Copyright Act, in cases where originality requirements are unfulfilled and large amounts of data have been compiled, the person making such a catalogue, program or table has the exclusive right to control the whole or a substantial part of the database.

Potential issues

In 1989, a WIPO Committee of Experts concluded that the only mandatory requirement for a literary or artistic work to be protected by the Berne Convention is that it must be "original". Some commentators have opined that certain non-SQL structured collections of data – the kind that might be produced by text and data mining (TDM)[13] systems – may not technically qualify for copyright protection as "databases" and that the data captured for use by AI systems fails to meet the requisite requirements for originality (Tariq 2020, Gervais 2019).

The concern lies in that copyright and other rights in databases may create a barrier to TDM systems whose operations may infringe on such rights, as the protection of the database as a collection does not extend to the underlying data as per Article 10(2) of the TRIPS Agreement, which reads: "Compilations of data or other material, whether in machine-readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself shall be without prejudice to any copyright subsisting in the data or material" (Rubinfeld and Gal 2016). This means that copyright works – such as images, texts, musical works and other copyright subject-matter – reproduced in a Big Data corpus retain independent copyright protection and

12 *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991).

13 Data mining is the process of finding styles and extracting useful statistics from large datasets. Text mining is an AI technology that entails processing facts from numerous textual content files.

that only TDM tools involving minimal copying of a few words or crawling through data and processing each item separately could be operated without running into a potential liability (Geiger et al. 2019).

The UK provides a TDM exemption in the form of a right to make a copy of a work "for computational analysis of anything recorded in the work". More specifically, Sec. 29A of the CDPA permits copying for non-commercial research, as long as the copy is accompanied by a sufficient acknowledgement (unless this would be impossible for reasons of practicality or otherwise) but requires authorisation from the copyright holder for other uses. Whether such a TDM exception is liable to cause an unreasonable loss of income to copyright holders is uncertain, but some academics have endorsed the UK Government's Licensing Framework that allows a degree of open access to government works, thereby helping to ensure that more members of the public have access to any new works created (Okediji 2016).

UK policymakers may also want to keep abreast of related developments elsewhere involving TDM, such as Google's recent announcement of licensing deals with Australia's Seven West Media group, Nine Entertainment and News Corp to pay for news content (Kaye 2021, Meade 2021, Samios 2021).

Data curation

Data curation, defined as the active and ongoing management of data through its lifecycle of interest and usefulness, and the need for better quality curation is growing given requirements for future legal compliance – for example, to ensure that data, with respect to data-protection laws, does or does not fall within the definition of "biometric data" or "biometric information" for the threshold conditions for legal protections to apply (Horowitz 2019, Kak 2020). There is considerable skill involved in data curation (as evidenced, inter alia, by data curation courses taught at various tertiary institutions) but the ability to protect the related IP is limited, though some patents on data curation do exist (e.g. US9542412B2 "Method and system for large-scale data curation" and WO2019173860A1 "Method and system for data curation").

Shared IP

There are strong reasons for AI developers to share IP given the potential benefits of collaboration. Patent pools, in general, allow multiple firms to draw on their strengths to produce a complex piece of technology. Companies including Microsoft, Intel, and Dell frequently collaborate to develop improved computer systems, and independent developers work with Apple to create iPhone mobile applications. By taking advantage of another company's experience, inventors can develop new products faster and cheaper than they would if they had to start from scratch.

With regards to the UK, Sec. 36 Patents Act 1977 provides every co-owner the right, subject to an agreement to the contrary, to exploit the patent itself, but it must obtain the other owner's consent (a) to amend or revoke the patent, (b) to grant a license under the patent, or (c) to assign or mortgage its share of the patent. In addition to the traditional

potential problems of joint IP ownership (O'Connell 2011), other issues potentially arise where jointly developed AI inventions are concerned, not only from shared data (e.g. privacy, bias) but also if AI is used by one or more parties – for example, if one party employs AI and creates more IP than the other party, feelings of inequity may arise; or if multiple AI are used and interact with each other, it may be difficult to determine IP ownership if parties choose to segregate rather than pool ownership.

6 TRADE

The development of AI raises IP and international trade issues as AI relies on large amounts of input data and data flows are thus a critical concern not just for training data purposes, but also to conduct remote (and cross-border) technical meetings and other collaborative activities. It is therefore useful to review the data-related aspects of major recent trade agreements.

As noted earlier, the WTO framework was created not only before technological breakthroughs on AI but even before the advent of global e-commerce. These technological and commercial developments have highlighted the shortcomings of the multilateral trading system – for example, in deciding whether businesses offering goods such as MP3 files or e-books over the internet should be subject to the GATS, GATT, or both (Wu 2017).

The WTO's attempt to grapple with the challenge posed by socio-technological change through an Electronic Commerce Work Programme have largely been in vain and many issues remain unresolved (Liu and Lin 2020). This has led WTO members to attempt to close gaps with FTAs.

The CPTPP is the largest and most representative agreement covering data-related issues to date. Like most comprehensive agreements, the CPTPP includes provisions on cross-border data flows and personal information protection that "allow the cross-border transfer of information" subject only to restrictive measures being taken for a "legitimate public policy purpose" so long as the restrictions are not discriminatory or disguised trade barriers. The CPTPP also prohibits localisation requirements for computing facilities, with a similar public policy exception. While the addition of public policy exceptions is understandable and likely essential, they are subject to abuse and therefore provisions enabling the flow of cross-border data and the prohibition against data localisation are not completely guaranteed.

The CPTPP also contains provisions which prohibit signatories from requiring the transfer or access to source code of software owned by a person of another Party "as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory" as well as forced technology transfers; prohibit customs duties

on digital trade (such as music, entertainment, software and games);[14] provide for non-discriminatory treatment of digital products; and require signatories to maintain a legal framework governing electronic transactions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the UN Convention on the Use of Electronic Communications in International Contracts 2005. It also includes provisions relating to electronic authentication and electronic signatures, spam, paperless trading and online consumer protection.

The CPTPP also contains provisions mandating strong copyright protection (including anti-circumvention of technological protection measures) but equally wide exceptions for purposes such as criticism, comment, news reporting, teaching, scholarship, and research. Importantly for AI, the treaty explicitly makes these exceptions applicable in the digital environment, and provides 'safe harbour' provisions so that internet service providers can escape liability for copyright infringement without the need to monitor their systems.

Following the negotiation of the CPTPP, similar hard rules on data flows were incorporated in numerous trade agreements, largely with the same or extremely similar wording.[15] The USMCA, which entered into force on 1 July 2020, likewise contains prohibitions on local data storage; robust IP and trade secret protections; provisions on cybersecurity, customs duties, electronic authentication, personal information and privacy, spam, access to government data, and liability for internet platforms. It also includes provisions that could be particularly helpful to American tech companies, as the removal of foreign digital trade barriers should allow these companies to achieve economies of scale by preventing countries from blocking them from using cloud computing to aggregate and analyse global data, thereby enabling them to amass huge amounts of data.

Of note, the USMCA is the first agreement to explicitly include protection for "an algorithm expressed in that source code", with the agreement defining an algorithm as "a defined sequence of steps, taken to solve a problem or obtain a result". While some commentators believe the addition of algorithm protection redundant and already covered under the term "source code", this is a narrow view. While the source code is the expression of an algorithm, it may be expressed in a different format and therefore appear to be very different. As a simple example demonstrating the difference, consider an algorithm to be the equation "5 + 10 = 15". This may be expressed in source code as "Z = Y + X". Unsurprisingly, the USMCA has been used as a blueprint for subsequent US trade agreements and its key provisions are mirrored in the October 2019 Digital Trade Agreement between the US and Japan.

14 The prohibition on customs duties is different from a tax on the sale of goods online. The latter is allowed by the US and currently 27 American states impose taxes on goods sold through the Internet, a recent trend as a result of the US Supreme Court decision in South Dakota v. Wayfair, Inc. 585 U.S. ___ (2018), which established that individual states can require e-commerce retailers to collect state sales tax on the goods they sell even without a physical presence in the state.

15 Examples include FTAs between Chile and Uruguay (2016), Singapore and Australia (2016 updates), Argentina and Chile (2017), Singapore and Sri Lanka (2018), Australia and Peru (2018) and Australia and Indonesia (2019).

The US approach to FTAs has also influenced the UK, which has adopted an approach more closely aligned with the US, thereby shifting away from the EU's approach to data (Irion and Williams 2019). For instance, in the UK–Japan Comprehensive Economic Partnership Agreement (CEPA) – the UK's first agreement signed independently from the EU – the parties agreed to prohibit restrictions on the cross-border data flows (including personal data) for the conduct of business or impose data localisation requirements (echoing the wording in Art. 19.12 of the USMCA). Both provisions contain an exception for measures undertaken to pursue a "legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade", and the provision on cross-border data flows contains an additional qualifier that the measure "does not impose restrictions on transfers of information greater than are required to achieve the objective".

While these two provisions have become commonplace in modern trade agreements, this is a first for the UK as the EU has been unwilling to agree to such commitments given its approach to data protection as expressed in the General Data Protection Regulation (GDPR). Instead, the EU seeks to ensure citizen's personal data is adequately protected in the destination country by requiring an "adequacy decision" which ensures protection to a level equivalent to the GDPR.

The UK–Japan CEPA also prohibits the mandatory transfer or access to source code ("or an algorithm expressed in the source code" with an algorithm defined as "a defined sequence of steps, taken to solve a problem or obtain a result", echoing the wording in Art. 19.16.1 of the USMCA) and provisions to shield cryptography from a very broad range of government requirements – including having to share and disclose keys or underlying technology or production processes, but also being forced to use specific technology. The agreement likewise prohibits the imposition of customs duties and contains provisions on the non-discrimination of domestic regulation, no prior authorisation requirement, e-transactions and signatures, consumer and personal information protection, spam and open government data (encouraging the release of anonymised government datasets where appropriate).

With respect to IPRs, the CEPA goes further than EU FTAs in that it introduces provisions on the enforcement of IP in the digital environment. Here again, the UK is following the US model by establishing a 'safe harbour' provision for online service providers to escape liability for the infringing activities of users and requiring online service providers to disclose expeditiously to a right holder "information sufficient to identify a subscriber whose account was allegedly used for infringement", with the added safeguard that such measures should avoid becoming a barrier to legitimate conduct. The CEPA differs from US agreements in that it is not prescriptive as to how each party should effectuate the provisions of the agreement. Moreover, the CEPA does not include any general rules governing the liability of internet platforms, which seems to be a conscious omission given the lack of consensus at the domestic level on this issue.

Therefore, while the CEPA largely follows the US blueprint, it does deviate to some extent in the wording of several key provisions and with respect to IPRs in the level of detail and prescription required from each party. The CEPA also seems to allow for wider scope of exceptions, including arguably broader exceptions for disclosure of source code and algorithms.

Meanwhile, the EU–UK Trade and Cooperation Agreement (TCA) represents the first time the EU has a chapter dedicated solely to digital trade. The chapter sets out preferential arrangements in areas such as trade in goods and in services and digital trade, before providing for a right to regulate for legitimate policy objectives. The chapter also prohibits the requirement to use computing facilities in a party's territory including by imposing certification requirements for such facilities; the forced localisation of data in a party's territory; the prohibition of storing and processing data in the other party's territory; and other restrictions making cross-border transfers dependent on the use of computing facilities in the party's territory. The TCA also prohibits customs duties for electronic transmissions, the mandatory transfers of source code (algorithms are not mentioned in the chapter) and prior authorisation, while also addressing issues relating to consumer protection. The TCA is, however, more limited in scope and complexity than the UK–Japan CEPA.

This is not surprising given the EU's reluctance to comprehensively address cross-border data flows for fear of the provisions being incompatible with the GDPR. The EU's policies on data transfer place a strong emphasis on privacy and these are reflected in its FTAs. While members of the EU can rely on legitimate interest disclosure provisions under Recital 47 of the GDPR to cover intra-EU transfer of data, there are strict regulations covering the transfer of personal data outside the EU, particularly given that many non-EU countries do not have similar legitimate disclosure provisions in their laws. In this regard, EU FTAs are more limited than those of other countries.

For example, the EU–Japan Economic Partnership Agreement (EPA) recognises the importance of technological neutrality; prohibits the mandatory transfer or access to source code (with no mention of algorithms and few listed exceptions); requires reasonable, objective and impartial domestic regulation, no prior authorisation; covers electronic authentication methods and electronic signatures; and includes provisions on consumer protection, spam and cooperation. Importantly, the agreement fails to mention data localisation and simply states that parties "shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data". The EU–Mexico Global Agreement looks very similar in all respects, including the call to reassess the need for a provision on data flows. However, it contains a more detailed list of exceptions to the prohibition on the transfer of source code in a manner more similar to US and UK agreements. With regards to intellectual property, the EU FTAs do not contain any technology-specific provisions, and in this respect have veered significantly from agreements negotiated by the US and others.

Looking at the situation from an AI perspective, the UK is wise to depart from the EU model and veer towards a more open approach to digital trade, given the UK's need for and reliance on imported data. While personal data of citizens is obviously important, the GDPR has potentially restricted innovation and technology access and creates roadblocks for European companies looking to embrace AI as well as blockchain and data storage. The GDPR has also led to unintended consequences, including enormous compliance costs for companies (with SMEs particularly burdened).

Other more recent EU initiatives also potentially have market-distorting consequences and, while part of domestic law, they would either be included in or limit the scope of what could be negotiated in a trade agreement. For example, the EU's so-called Right to Repair requiring technology to last a decade is well meaning in that it is designed to reduce waste, but the commercial impact on firms supplying underlying AI systems – for example, being forced to support products they abandoned or obsolete technologies – is undetermined (Smith 2021).

Another example is the European Commission's call for developers to disclose the design parameters and metadata of datasets in the event of accidents caused by AI systems as a means of improving transparency of algorithms, since the 'black-box effect' in AI systems makes it difficult for users to trace the decisions made about them by such systems. (European Commission 2020b). This conclusion seems short-sighted and misguided, given that aside from the aforementioned issues of AI algorithmic unpredictability, problems arising from the performance of AI systems may result from the data used for training or operations, not the algorithms themselves (Korolov 2018). Moreover, given that technology vendors view this information as trade secrets and go to great lengths to guard it with non-disclosure agreements, physical security and access control mechanisms and even rapid updates (Google, for instance, made 3,234 updates to its search algorithms in 2018), such a scheme would undoubtedly reduce the attractiveness of the UK as an investment location for an AI company (Meyers 2019).

7 RECOMMENDATIONS

7.1 Common definition of AI

The UK should adopt a common definition of AI and AI-related terms, particularly for formulating innovation, IP and trade policies for AI. Such a definition would ensure that the UK can formulate domestic policy through a comprehensive, holistic and coherent approach and that it and its trading partners can enter negotiations with the same expectations and understandings on the subject matter potentially covered by the term 'AI'.

7.2 Securing access to data is critical and should be a high priority

This chapter made it clear that AI systems require large datasets to initialise and data is needed for successful product localisation. Here, quantity matters because AI, and in particular ML, must be able to incorporate into future predictions as many past outcomes as possible. This means that access to the tails of data – less usual and irregular data – matters. For a country the size of the UK, access to data is critical to any aspirations the nation has in AI development.

What tends to be overlooked, however, is how important data and access to data is for the competitiveness of companies. Data and access to data can provide useful market insights. Consider Amazon's use of an AI-powered product search engine to glean insights about products customers want that it may not even sell, based on the searches of hundreds of millions of customers (Dunne 2020). By leveraging the data, Amazon can offer similar products and promote them on its site, and even advertise them on Google using the same keywords shoppers use on Amazon.

With all this in mind, access to data should be a high priority in any trade negotiation. While the focus to date has largely been on infrastructure location, which mostly affects costs for companies and users (who ultimately have to shoulder the extra expense), access to data has implications for the development of AI and AI-based services and the competitiveness of UK companies operating or seeking to operate in the space. For this reason, initiatives which could hamper the transfer of data or the attraction of the UK as an AI development centre (such as those being promulgated by the EU) should be avoided. The UK should continue to adopt a US-style approach to digital trade and IP chapters in subsequent trade agreements. This may not be so easy in the future, however, as the UK will inevitably have to deal with jurisdictions with a 'less free' approach to internet governance and digital trade (Benvenisti 2018). Some negotiating partners may insist on strict data and infrastructure localisation requirements, which will run counter to the UK's priority of securing access to local data. While China is not alone in this approach, it is useful to use it as an example. China's Cybersecurity Law requires operators of critical information infrastructure to store all personal information and important data gathered or produced within the territory within Mainland China. This law cannot be avoided by means of an FTA. It is not only China, of course, and according to the latest Freedom House report, two-thirds of the global internet population are in countries deemed "not free" or "partially free", freedom on the Internet has decreased, and the slow-motion "splintering" of the internet has transformed into an all-out race towards "cyber sovereignty" (Freedom House 2020). In the near future, the UK will be negotiating with countries whose regimes more closely resemble that of China than, say, Japan, which led G20 countries in the ease of cross-border data flows according to a 2019 Salesforce report on Internet freedom (Salesforce 2019). This situation will require negotiations for specific carve-outs in certain areas.

7.3 Intellectual property and AI

While it is important for policymakers to be cognizant of the IP issues mentioned throughout this chapter, TDM-related IP matters tend to be overlooked. A sudden curtailment of information due to IP infringement would profoundly impact AI systems and developers. For this reason, matters regarding TDM and the protection of copyright content contained within databases should be given more attention, and UK policymakers/negotiators should seek to negotiate clear and broad exceptions for TDM in subsequent FTAs. The UK would also be wise to continue providing for IP-like protection for algorithms and for the inclusion of 'safe harbours' for online service providers in its FTAs.

At the same time, while there may be a temptation to amend domestic IP laws in order to encourage investment, policymakers might wish to heed the experiences of other jurisdictions. For example, while some have claimed that the US' more permissive software patenting regime is a primary reason why more software development took place in the US than Europe, (Guntersdorfer 2003, Yoches et al 2011), this may be overstated. To illustrate, when the US Supreme Court decision in *Alice Corp. v. CLS Bank International*[16] effectively raised standards of patentability for software[17] and the US Patent and Trademark Office (USPTO) responded by issuing new guidelines increasing the burden on applicants to provide a more robust disclosure for computer-related claims, the US did not see an outflow of investment, innovation or talent. Similarly, the 2018 report on the impact of the Database Directive made no mention of any great new flows of technological investment into the EU as a result of the Directive. (European Commission 2018b) It is likely that carefully drafted and targeted provisions in FTAs will achieve the IP policy objectives and thus ought to be considered ahead of amendment of IP laws.

7.4 Impact of other related laws and regulations

This chapter has illustrated the unintended consequences of several EU laws and regulations. Non-trade-related laws that seek to regulate AI in some manner can, and often do, have negative impacts not only elsewhere but also on the domestic industry. Policymakers and trade negotiators must be aware of the potential consequences of non-trade-related laws and regulations to ensure they do not damage the industry in an unintended manner.

16 *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014).
17 The court avoided providing a clear definition of the expression "software patent" and held that "merely requiring generic computer implementation fails to transform [an] abstract idea into a patent-eligible invention".

7.5 Investment in innovation

Given the UK's relatively small domestic population, it should invest in and investigate technology to build AI systems that are less reliant on large datasets (and therefore imported data) – for example one-shot learning, dataset distillation, and synthetic data – in order to make the best use of its abilities and resources.

REFERENCES

Arntz, M, T Gregory and U Zierahn (2016), "The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis", OECD Social, Employment and Migration Working Papers No. 189 (http://dx.doi.org/10.1787/5jlz9h56dvq7-en).

Australia Department of Industry, Science, Energy and Resources (2020), "Mapping Australia"s Artificial Intelligence and Autonomous Systems Capability", December (https://consult.industry.gov.au/digital-economy/mapping-australias-ai-capability/).

Barfield, W (2018) "Towards a law of Artificial Intelligence", in W Barfield and U Pagallo (eds), Research Handbook on the Law of Artificial Intelligence: 2.

Benvenisti, E (2018), "Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?", 29(1) *European Journal of International Law* 9–82.

Brynjolfsson, E, D Rock, and C Syverson (2017) "Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics, NBER Working Paper No. 24001, (http://ide.mit.edu/sites/default/files/publications/erik%20paper_0.pdf, November).

Calo, R (2018), "Artificial Intelligence Policy: A Primer and Roadmap", 51 *UC Davis Law Review* 399.

Chessen, M (2017), "What is Artificial Intelligence? Definitions for policy-makers and non-technical enthusiasts", *Medium*, 3 April (https://medium.com/artificial-intelligence-policy-laws-and-ethics/what-is-artificial-intelligence-definitions-for-policy-makers-and-laymen-826fd3e9da3b).

China State Council (2017), "New Generation of Artificial Intelligence Development Plan", State Council Document [2017] No. 35 (https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf).

Davies, C R (2011), "An evolutionary step in intellectual property rights – Artificial intelligence and intellectual property", Computer Law & Security Report, 27 December.

Debussche, J and J César (2019), "Big Data & Issues & Opportunities: Intellectual Property Rights", Bird & Bird, March (www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-ip-rights).

DACS – Design and Artists Copyright Society (2018), "Copyright Uncovered: Fair Use v Fair Dealing" (www.dacs.org.uk/latest-news/copyright-uncovered-%E2%80%93-q3-2018-fair-use-v-fair-deal?category=For+Artists&title=N).

Drayson, P (2019), "Britain needs to step up to win the global AI healthcare race", *City A.M.*, 7 January (www.cityammckins.com/britain-needs-step-up-win-global-ai-healthcare-race/).

Dunne, C (2020), "Amazon A10 Algorithm: Everything You Wanted to Know" (https://blog.repricer.com/resources/amazon-a10-algorithm/).

European Commission (2018a), "Artificial Intelligence For Europe", Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, SWD(2018) 137 final, April.

European Commission (2018b), "Evaluation of Directive 96/9/EC on the legal protection of databases, Brussels 25.4.2018 (European Commission 2018B)", 25 April.

European Commission (2020), "On Artificial Intelligence - A European approach to excellence and trust", 19 February (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf).

European Commission (2020), "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics", Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, 19 February (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en).

European Commission (2021), "A European approach to Artificial intelligence", High-Level Expert Group on Artificial Intelligence, March (https://ec.europa.eu/digital-single-market/en/artificial-intelligence).

Fleuter, S (2016), "The Role of Digital Products Under the WTO: A New Framework for GATT and GATS Classification", 17 *Chicago Journal of International Law* 153.

Freedom House (2020, "Freedom on the Net" (https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf).

General Agreement on Tariffs and Trade (1947), 61 Stat. A-11, 55 U.N.T.S. 194, 30 October.

General Agreement on Trade in Services (1994), Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 15 April.

Geiger, C, G Frosio and O Bulayenko (2018), "Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data?", 48 *International Review of Intellectual Property and Competition Law* 814.

Gervais, D J (2019), "Exploring the Interfaces Between Big Data and Intellectual Property Law", 10 *Journal of Intellectual Property* 22.

Gonfalonieri, A (2019), "5 Ways to Deal with the Lack of Data in Machine Learning", KD Nuggets, June (www.kdnuggets.com/2019/06/5-ways-lack-data-machine-learning.html).

Gurkaynak, G, I Yılmaz, T Doygun, and E Ince (2018), "Questions of Intellectual Property in the Artificial Intelligence Realm", 3 *The Robotics Law Journal* 9.

Guntersdorfer, M (2003), "Software Patent Law: United States and Europe Compared" (https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1075&context=dltr).

Hart, T (2018), "Secret History of Copyright: NAFTA, USMCA, and Fair Use", Copyright Alliance Blog, 20 November (https://copyrightalliance.org/nafta-intellectual-property/).

Heckman, J R, E L Boehmer, E H Peters, M Davaloo, N G Kurup (2015), "A Pricing Model for Data Markets", *iConference 2015 Proceedings* (www.ideals.illinois.edu/bitstream/handle/2142/73449/207_ready.pdf?sequence=2).

Hervey, M (2021), "UKIPO patent guidance updated for DABUS judgment", 8 January (https://loupedin.blog/2021/01/ukipo-patent-guidance-updated-for-dabus-judgment/).

Higgins, B (2020), "First They Wanted Data, Now Cyber Thieves Are After Deep Learning Models: Legal Response Options", *Artificial Intelligence Technology and the Law*, 8 January (https://aitechnologylaw.com/2020/01/now-cyber-thieves-want-your-deep-learning-model/).

Hippold, S (2020), "6 AI Myths Debunked", Gartner, 13 November (www.gartner.com/smarterwithgartner/ai-myths-debunked/).

Horowitz, B M (2019), "Implementations of Cyber Attack: Resilience Solutions for Cyber Physical Systems" in William Lawless et al. (eds.), *Artificial Intelligence for the Internet of Everything*, pp. 87-100.

House of Lords Select Committee on Artificial Intelligence (2019), *AI in the UK: Ready, Willing and Able?*, Report of Session 2017–19 (https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf).

Irion, K and J Williams (2019), "Prospective Policy Study on Artificial Intelligence and EU Trade Policy", The Institute for Information Law.

Kahneman, D (2011), *Thinking, Fast and Slow*, Farrar, Straus and Giroux.

Kak, A (2020), "The State of Play and Open Questions for the Future", AI Now Institute, 2 September https://ainowinstitute.org/regulatingbiometrics-kak.pdf).

Kaye, B (2021), "Australia"s Seven West Media strikes deal with Google for news", Reuters, 15 February (www.reuters.com/article/us-australia-media-google-seven-west-med-idUSKBN2AE0TK).

Kemp, R (2020), "UK: Algo IP: Intellectual Property In Algorithms, Computer Generated Works And Computer Implemented Inventions", 12 June (mondaq.com/uk/patent/952154/algo-ip-intellectual-property-in-algorithms-computer-generated-works-and-computer-implemented-inventions).

Klein, M (2020), "50 Million Join The 'Creator Economy; Thanks To Platforms Like Only Fans, YouTube, Etsy And Twitch", *Forbes*, 23 September (www.forbes.com/sites/mattklein/2020/09/23/50m-join-the-creator-economy-as-new-platforms-emerge-to-help-anyone-produce-content--money/?sh=593a9223165f).

Korolov, M (2018), "AI's biggest risk factor: Data gone wrong", *Insider Pro*, 13 February (www.idginsiderpro.com/article/3254693/ais-biggest-risk-factor-data-gone-wrong.html).

Lee, K F (2018), "Why China Can Do AI More Quickly and Effectively Than the US, The US may be leading the discoveries in AI—but Chinese entrepreneurs are better at implementing them", *Wired*, 23 October (www.wired.com/story/why-china-can-do-ai-more-quickly-and-effectively-than-the-us/).

Liu, H W and Lin, C F (2020), "Artificial Intelligence and Global Trade Governance: A Pluralist Agenda", 61(2) *Harvard International Law Journal* 407

MIT Laboratory for Information and Decision Systems (2020), "The Real Promise of Synthetic Data", *MIT News*, 16 October (https://news.mit.edu/2020/real-promise-synthetic-data-1016).

Meade, A (2021), "Nine agrees to join Google News Showcase in Australia for reported $30m a year", *The Guardian*, 17 February (www.theguardian.com/media/2021/feb/17/nine-agrees-to-join-google-news-showcase-in-australia-for-reported-30m-a-year).

Meyers, P J (2019) "How Often Does Google Update Its Algorithm?", *Moz*, 4 May (https://moz.com/blog/how-often-does-google-update-its-algorithm).

MBZUAI (2020), "'AI is the new electricity' – Dr. Kai-Fu Lee Explores the Evolution of Artificial Intelligence", MBZUAI Talks, December (https://mbzuai.ac.ae/news-events/MBZUAI-Talks-Dr-Kai-Fu-Lee-Explores-the-Evolution-of-Artificial-Intelligence).

McKinsey Global Institute (2019), *Artificial intelligence in the United Kingdom: Prospects and challenges*, June (www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Artificial%20intelligence%20in%20the%20United%20Kingdom%20Prospects%20and%20challenges/Artificial-intelligence-in-the-United-Kingdom-VF2.ashx).

Meltzer, J P (2018), "The impact of artificial intelligence on international trade", Brookings, 13 December (www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/).

Marcus, G (2018), "Deep Learning: A Critical Appraisal", arXiv:1801.00631 [cs.AI], 2, January.

National Science and Technology Council Committee on Technology (2016), "Preparing for the Future of Artificial Intelligence", October (https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf).

O'Connell, D (2011) "Avoid jointly owned intellectual property" (www.ipeg.com/avoid-jointly-owned-intellectual-property/).

Okediji, R L (2016), "Government as Owner of Intellectual Property? Considerations for Public Welfare in the Era of Big Data", 18(2) *Vanderbilt Journal of Entertainment & Technology Law* 331.

Ransbotham, S, D Kiron, P Gerbert and M Reeves (2017), "Reshaping Business With Artificial Intelligence: Closing the Gap Between Ambition and Action", 59(1) *MIT Sloan Management Review*.

Rubinfeld, D L and M Gal (2016) "Access Barriers to Big Data", 59 *Arizona Law Review* 339.

Salesforce (2019), "Japan Leads G20 Countries in Cross-Border Data Flows – New Salesforce Study Finds", 24 June (www.salesforce.com/news/stories/japan-leads-g20-countries-in-cross-border-data-flows-new-salesforce-study-finds/).

Samios, Z (2021), "Rupert Murdoch"s News Corp signs global news deal with Google", *Sydney Morning Herald*, 18 February (www.smh.com.au/business/companies/rupert-murdoch-s-news-corp-signs-global-news-partnership-deal-with-google-20210218-p573j6.html).

Schwartz, B (2020), "Bing does now know how its ranking signal weights - machine learning deals with it", Search Engine Roundtable, 10 November (www.seroundtable.com/bing-ranking-signal-weights-machines-learning-30404.html?utm_campaign=TodayInDigital.com)

Sergeev, A (2017), "Volvo"s Autonomous Tech Can"t See Bouncing Kangaroos", *Motor1*, 28 June (www.motor1.com/news/149687/volvo-autonomous-system-not-seeing-kangaroos/).

Singapore Personal Data Protection Commission (2020), "Model Artificial Intelligence Governance Framework Second Edition", January (www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf).

Smith, A (2021), " New EU Right to Repair laws require technology to last a decade", *Independent*, 2 March (www.independent.co.uk/life-style/gadgets-and-tech/eu-right-repair-technology-decade-b1809408.html).

Sobel, B (2017), "Artificial Intelligence"s Fair Use Crisis", *Columbia Journal of Law & the Arts* 45: 68-71.

Sucholutsky, I and M Schonlau (2020a), "Soft-Label Dataset Distillation and Text Dataset Distillation", 5 May (https://arxiv.org/abs/1910.02551).

Sucholutsky, I and M Schonlau (2020b), "Less Than One"-Shot Learning: Learning N Classes From M<N Samples", 17 September (https://arxiv.org/abs/2009.08449v1).

Surden, H (2014), "Machine Learning and Law", 89 *Washington Law Review* 87, 88.

Tariq, M (2020), "Compare difference between text and data mining", *AI Objectives*, 14 October (http://www.aiobjectives.com/2020/10/14/compare-difference-between-data-mining-and-text-mining/).

UK Department of Business, Energy and Industrial Strategy (2021), "The Grand Challenges", Policy Paper, 26 January (www.gov.uk/government/publications/industrial-strategy-the-grand-challenges/industrial-strategy-the-grand-challenges#contents).

UK Intellectual Property Office, (2019) "Artificial Intelligence, A worldwide overview of AI patents and patenting by the UK AI sector", June (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf).

UK Office for Artificial Intelligence (2019), "Guidance: A guide to using artificial intelligence in the public sector", 10 June (www.gov.uk/government/publications/understanding-artificial-intelligence/a-guide-to-using-artificial-intelligence-in-the-public-sector#defining-artificial-intelligence).

UK Intellectual Property Office and Government Digital Service (2020), "Sui generis database rights from 1 January 2021", 30 January (www.gov.uk/guidance/sui-generis-database-rights-after-the-transition-period).

UNCTAD (2018), "Trade Negotiations: Next Frontier for Artificial Intelligence", 18 June (https://unctad.org/news/trade-negotiations-next-frontier-artificial-intelligence).

US Copyright Office (2021), *Compendium of The US Copyright Office Practices*, Third Edition, (www.copyright.gov/comp3/docs/compendium.pdf).

Wei, E (2020), "Seeing like an algorithm", 30 September (www.eugenewei.com/).

Wilson, H J, P R Daugherty and C Davenport (2019), "The Future of AI Will Be About Less Data, Not More", *Harvard Business Review*, 14 January (https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more).

WIPO (2021), Conversation on Intellectual Property and Artificial Intelligence, Third Session, WIPO/IP/AI/3/GE/20/INF/5, 8 January (www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_3_ge_20/wipo_ip_ai_3_ge_20_inf_5.docx).

WIPO (2020a), "Copyright in the Age of Artificial Intelligence", 5 February (www.copyright.gov/events/artificial-intelligence/agenda.pdf).

WIPO (2020b), "Artificial Intelligence and Intellectual Property Policy", revised May (www.wipo.int/about-ip/en/artificial_intelligence/policy.html).

Wu, M (2017), "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System", ICTSD E15 Initiative, November (https://e15initiative.org/publications/digital-trade-related-provisions-in-regional-trade-agreements-existing-models-and-lessons-for-the-multilateral-trade-system/).

Xu, L, M Skoularidou, A Cuesta-Infante, K Veeramachaneni (2019), "Modeling Tabular Data using Conditional GAN", 33rd Conference on Neural Information Processing Systems (NeurIPS 2019), (https://arxiv.org/pdf/1907.00503.pdf).

Yoches, E R, R M McNeill, E H Arner, E H Lim, C S Schultz and L J Thayer (2011), "How Will Patent Reform Affect the Software and Internet Industries?", *The Computer & Internet Lawyer* 28(12): 5

Yu, P K (2014), "Trade Agreement Cats and the Digital Technology Mouse" in B Mercurio and K J Ni (eds), *Science and Technology in International Economic Law: Balancing Competing Interests*, Routledge, pp. 187-210.

ABOUT THE AUTHORS

Bryan Mercurio is the Simon F.S. Li Professor of Law at The Chinese University of Hong Kong. He is a specialist in international economic law, with a particular expertise in the WTO law, fragmentation of international legal and financial regimes, and the intersection between trade, intellectual property and investment. Professor Mercurio is the author of Drugs, Patents and Policy: A Contextual Study of Hong Kong (Cambridge University Press, 2018), co-author of one of the most widely used case books on WTO law (Hart Publishing, 2018, 3rd ed) and co-editor of the leading collection on bilateral and regional trade agreements (Cambridge University Press, 2nd ed, 2016).

Ronald Yu started in the information technology sector before studying law. He is a U.S. Patent Agent, digital forensics examiner and has worked at IBM, FedEx, Hewlett-Packard and Wang Laboratories. Mr. Yu has also started companies involved in technical public relations, localization, technical writing and online education, and taught postgraduate and undergraduate classes in Intellectual Property Law in Information Technology, Patent law and Intellectual Property Strategy. Mr. Yu advised the Hong Kong government on its e-Cert Public Key Infrastructure, digital signature initiative and is currently conducting research on cross-border data flows at the Chinese University of Hong Kong.

CHAPTER 4

Source code disclosure: A primer for trade negotiators

Cosmina Dorobantu, Florian Ostmann and Christina Hitrova[1]
The Alan Turing Institute and the Oxford Internet Institute; The Alan Turing Institute; Technical University of Munich

1 INTRODUCTION

In 1982, Therac-25 appeared on the market and was immediately hailed as a state-of-the-art medical machine. Produced by Atomic Energy of Canada Limited and sold to hospitals in the US and Canada, Therac-25 delivered computer-controlled radiation therapy. It was the most technologically advanced radiation therapy machine in use at the time, admired for its precision and reliance on an onboard computer. And yet, between June 1985 and January 1987, Therac-25 overdosed six patients with radiation doses that were hundreds of times higher than normal. Some patients died, while others were severely injured. Detailed investigations of the accidents followed, and their conclusions were clear: the deaths and injuries of these patients were, in no small part, due to errors made in the source code underlying Therac-25's software (Levenson and Turner 1993).

Since the tragic accidents caused by Therac-25, the use of software has become much more widespread. Nowadays, software is an integral part of our lives. Lines of code determine the news that we read online, power the smart speakers in our homes, recommend some of the medical treatments we receive, and help us navigate unfamiliar roads. Areas of our lives that, only a generation ago, we could not imagine would be touched by code – from our friendships to our work meetings – are now increasingly curated by software-powered technologies.

Software doesn't only control the devices in our homes and pockets. Businesses also increasingly rely on software to design their products, improve their operations, manage their employees, and advertise the goods and services they sell. In 2019, software made up over 10% of the UK's gross fixed capital formation – approximately £40.9 billion (Office for National Statistics 2020). Even industries with low levels of digitisation – from agriculture, forestry, and fishing to construction and real estate – are now investing heavily in software development.

1 The authors would like to thank Alan Winters, Ingo Borchert, David Leslie, and Olivier Le Gouanvic for insightful comments and valuable suggestions.

Software's presence in our daily lives and business operations is not only set to continue; it is poised to increase. As networked computing, digital interconnectedness, cost-efficient data storage, ever-increasing computing power, and financial investments continue their upward movement, software will only grow in importance. This growth will present individuals and businesses alike with unprecedented opportunities as well as significant challenges.

Policymakers have the difficult task ahead of striking the right balance between realising the benefits that software brings and minimising the risks. This task becomes more daunting when considering the international dimension. Code can easily cross borders, but it is not just code, on its own, that companies export. Products and services that incorporate or rely on software are also traded internationally. From watches and cars to medical devices and financial products, traded goods and services increasingly have software embedded in them. Software's increasing presence in internationally traded goods and services makes it an international matter, affected by future trade negotiations.

Recent trade agreements – from the Japan–Mongolia Economic Partnership Agreement to the United States–Mexico–Canada Agreement – incorporate specific provisions related to source code. These provisions prohibit governments and their agencies from requiring "the transfer of, or access to, source code of software owned by a person of the other Party."[2] This general prohibition on public authorities requiring the transfer of, or access to, source code matters. On the one hand, it encourages international trade by reassuring foreign software developers that they will not have to disclose the source code underlying their products and services. On the other hand, this general prohibition, even when accompanied by extensive exemptions, places limitations on the powers of governments and their agencies to examine source code.

Trade negotiators are increasingly having to take a stance on whether a general prohibition on governments requiring access to source code is desirable in a trade agreement, and if so, which exemptions should accompany it. Deciding on the best course of action requires a solid understanding of what source code is, how it functions, what can go wrong with it, and when governments and their agencies may have legitimate reasons to implement measures aimed at source code accessibility. It also requires a general understanding of how source code disclosure has been handled in existing trade agreements and what the limitations of the previous approaches are.

Surprisingly little has been written to help trade negotiators navigate the tricky – and expanding – territory that software occupies in our lives and trade agreements. While several publications dedicate a few pages to provisions on access to source code (e.g. Guglya

2 The Appendix contains the text of articles from recent trade agreements related to source code. This citation is common to most articles reflected in the Appendix.

and Maciel 2016, Wu 2017, McCann 2019), to our knowledge, no publication presents a holistic picture of how recent trade agreements have handled source code disclosure and why such disclosure might be necessary.

This chapter aims to fill this gap and help trade negotiators build the knowledge they need to confidently handle provisions related to source code in future trade agreements. The first section provides an introduction to source code. It defines what source code is, discusses our ability to understand what a piece of code does, and raises awareness of the role of humans when things go wrong. The second section provides an overview of possible motivations for government-mandated source code disclosure requirements and the forms that such requirements can take. The third section examines how source code disclosure has been handled in recent trade agreements. The final section concludes.

2 SOURCE CODE: BASIC CONCEPTS

In this section, we define source code and provide an example of what lines of code look like. We introduce two programming approaches: the traditional top-down, rules-based approach; and the more recent bottom-up, machine learning-based approach. We give a sense of what we can and cannot understand by looking at a piece of code. Finally, we end the section by reminding the reader that code does not act on its own volition. When things go wrong, they often do so as a result of cognitive limitations, errors, negligence, or ill intent on the part of humans.

2.1 Definition

Source code refers to the lines of code written by programmers to instruct a machine to perform a given task. Source code is usually written in a text file, it is readable by humans, and it uses a programming language, such as Python, C++, Java, or R.[3] For example, the simple lines of code below are written in Python and instruct a computer to prompt a user to enter their age and to convert the entered value into an integer number. If the resulting number is equal to or greater than 18, the code instructs the computer to display the message "You can vote in UK elections." If it is below 18, the computer will display the message "You cannot vote in UK elections."

```
age = int(input("Enter your age "))
if age >= 18:
       print("You can vote in UK elections")
else:
       print("You cannot vote in UK elections")
```

3 There are numerous other programming languages available.

Source code exists on a continuum, ranging from very simple code, like the lines above, to highly complex code. Pieces of code that contain a series of steps that need to be followed in order to solve a computational problem are often called algorithms.

2.2 Programming approaches

The traditional way of programming relies on explicitly programmed rules. Returning to the simple example above, if we wanted to produce a piece of code that lets a user know whether they are old enough to vote in the UK elections, we would rely on the top-down application of logical statements and rules, such as 'if this person's age is greater or equal than 18, then display the message "You can vote in UK elections"'.

A newer and more powerful way of programming relies on machine learning. In contrast to more traditional approaches, machine learning systems rely on data to 'learn' how to carry out a certain task in a bottom-up, inductive way, rather than being explicitly programmed to follow a set of predefined rules (Leslie et al. 2020: 36). For example, if we wanted to produce a piece of code that correctly identifies a dog in an image, instead of explicitly programming rules that describe what a dog looks like, we can write a piece of code that 'learns' what a dog looks like by identifying patterns that arise across the repetitious processing of thousands of labelled images.

The growing popularity of machine learning approaches is due, in no small part, to their ability to extract relevant features and properties from large datasets. To carry on with the dog image example further, in the past, creating a computer programme that had hard-coded rules of what a dog looked like was a monumental task. Dogs come in many shapes and sizes – a giant schnauzer, for example, looks very different from a westie. Pictures differ, too. Some pictures might be close-ups of a dog's face, while others might be landscape views of dogs running across a field. Some pictures might have good lighting, while others might have significant shading – or worse yet, other animals or people in them. While our human brains find it easy to recognise a dog in each one of these situations, it is difficult for human programmers to specify explicit rules that, when embedded in code, would equip a computer program with the same recognition capabilities. Machine learning has helped to solve this problem for us. Instead of requiring hard-coded rules of recognition, machine learning algorithms extract the relevant features and properties of what a dog looks like from large datasets.[4] This is a powerful and transformative technology that is fundamentally different in its approach from top-down, rule-based programming.

The reliance of bottom-up approaches on a 'learning' process gives rise to a consequential difference between them and top-down approaches. When it comes to the design of a system, what matters in top-down approaches is the way in which expert knowledge is translated into specific rules. In machine learning approaches, the 'learning' process is

4 For readers interested in the history, development, and risks of facial recognition technologies, Leslie (2020) provides an excellent review.

what guides a system to extract relevant information from the data. Questions such as 'how do we pick an appropriate target variable?', 'how do we choose the input variables that the system relies on?', and 'how do we model the relationship between the input variables and the target variable?' are of paramount importance in machine learning. The answers to questions like these form the basis for arriving at the mathematical formulation that underpins the machine learning system. We refer to this as the system's 'logic' or rationale. When we try to understand the inner workings of a machine learning system, it is extremely useful if, in addition to the source code, we also have access to an expression and elucidation of the system's underlying rationale.

2.3 Understanding what a piece of code does

There is a vast literature on the difficulties, limitations, and methodologies for analysing source code. We don't replicate that body of knowledge here, but instead summarise some of the key points on which this literature agrees.[5]

First, there are two ways of examining code. One is through static analysis, which consists of analysing the code without running it. The other is through dynamic analysis, which entails observing the code 'in action' by running it and analysing its outputs.

Second, the complexity of the code affects our ability to ascertain how it functions. The lines of code at the beginning of this section are easy to interpret. A simple, static analysis reveals how the inputs (the user's age) are turned into outputs (a message that tells the users if they can vote in UK elections). If, however, we were to examine highly complex code, such as the code that a search engine uses to rank results, it would be a monumental task to ascertain how the code generates the search results that a user sees for a given query. Such an examination would necessitate a dynamic analysis and the results of even the most thorough analysis would have limitations. For some highly complex machine learning systems, a complete understanding is impossible to achieve.

Finally, although a complete understanding of a given piece of software may be difficult or impossible to achieve, having access to the source code can make a big difference. For any software, ranging from the simplest to the most complex, we are able to paint a much clearer and fuller picture of how it functions – or malfunctions – if we can analyse the underlying code. In many situations, source code analysis can be an indispensable component for developing a sufficiently detailed understanding of how the software functions.

2.4 The role of humans when things go wrong

In 2020, GCSE and A-level examinations were cancelled due to the Covid-19 pandemic. Ofqual, the organisation tasked with regulating qualifications, exams, and tests in England, decided to produce an algorithm that would compute an exam grade for each

5 Some of the prior literature on this topic is written for a general audience (e.g. CMA 2021), while other parts of it are written for an academic audience (e.g. Desai and Kroll 2018).

student. The intention was for the algorithm to ensure that qualification standards were maintained and that grade inflation was kept under control. Yet, when students received their algorithmically generated results, it started to become clear that the code was more likely to award higher grades to children from private schools and lower grades to children from state schools. Faced with a growing public backlash, the government decided against using the grades generated by the algorithm. As the dust started to settle on the exam grade fiasco, the prime minister visited Castle Rock High School in Coalville, Leicestershire. Addressing the assembled students, he said "I am afraid your grades were almost derailed by a mutant algorithm and I know how stressful that must have been" (Coughlan 2021).

As this quote illustrates, we have a tendency to think of code as having agency. We assign it human-like powers: we speak of algorithms that judge us, that lie to us, or that learn from us. When things go wrong, as they did last summer, we prefer to give code a life – and will – of its own: the algorithm went rogue or mutated, much like a living virus would when adapting to changing conditions.

Code, however, does not act on its own volition. It is written by humans,[6] according to specifications defined by humans. When things go wrong, our malicious intentions, errors, or limitations are often at play. In particular:

- **Software can be deliberately programmed to serve illicit purposes.** This is where malicious intentions are at play. Malware, for example, refers to code that is "specifically designed to disrupt, damage, or gain unauthorised access to a computer system."[7] Apart from malware, code can and has been used to evade existing standards, laws, and regulations. For example, engineers at Volkswagen and other car manufacturers specifically programmed code to manipulate the results of emissions tests.

- **Software can have unintended consequences.** This is where human errors and limitations come into play, despite our best intentions. We make mistakes when designing software, specifying the requirements, writing the code, and testing the performance of a programmed system. As the Therac-25 example shows, the errors that we make can have disastrous consequences. We also fail to foresee all the consequences or uses of a particular piece of code. Even when designed and developed in accordance with best practices, pricing algorithms that monitor and react to competitors' pricing strategies could, for example, lead to price collusion (Ezrachi and Stucke 2016). And well-intended software, like Microsoft's Twitter bot

6 Code can also be automatically generated now, but humans are very much involved there, too. It is humans that program how a system can generate code.

7 Source: Oxford Languages from Oxford University Press.

named Tay, can be sabotaged by Twitter users and turned into a sexist and racist chatbot – a far cry from Microsoft's original intention of having a friendly chatbot that would converse with millennials (Schwartz 2019).

The examples above shine light on our failings, as humans. We sometimes have malicious intentions. We make mistakes. We fail to foresee how a piece of code will behave when deployed – or how other human beings will interact with it. The code that we write and the software systems that we produce simply reflect these failings. As the prevalence of software increases, our ability to understand where humans made deliberate attempts to cause harm or unintended mistakes becomes ever more important. Source code disclosure can help build that understanding, making it an essential tool for the detection of foul play or negligence. This is one important reason, among others, why access to source code can be desirable in general, and why governments may choose to enact source code accessibility requirements in particular. We turn to a more comprehensive discussion of such reasons in the next section.

3 POSSIBLE SCENARIOS OF GOVERNMENT-MANDATED SOURCE CODE DISCLOSURE

The landscape of possible government-mandated requirements on technology providers to disclose source code can be surprisingly complex. The wide range of purposes that such requirements can serve and the fact that the disclosure itself can be made to a variety of recipients – inside or outside the government – contribute to that complexity. In this section, we consider the range of possible scenarios involving government-mandated disclosure of source code. The discussion is not meant to be exhaustive, but to provide an overview of the reasons for disclosure that have played a prominent role in policy discussions to date. These reasons can be structured around three main categories:

- meeting regulatory and judicial needs
- meeting procurement needs
- promoting innovation and economic development.

3.1 Meeting regulatory and judicial needs

Software is increasingly relevant to questions of regulatory compliance and lawfulness. The ever-expanding use of software in products and services means that countries' regulatory and judicial authorities face a growing number of situations where they need to determine whether software is consistent with regulatory or legal requirements. Conclusive assessments may require the analysis of source code and, even where they could in principle be achieved through other means, may prove cheaper and easier to

complete by accessing the source code. Governments may therefore establish rules and schemes that ensure that relevant authorities and actors related to them are able to access source code for purposes of assessing compliance and lawfulness.

Questions of compliance and lawfulness in relation to software arise in virtually every domain. The examples below serve to illustrate just how widespread these questions and concerns are.

Competition law. The way in which a piece of software is programmed can be central to different types of competition law violations. As an example, software can be used in ways that – intentionally or unintentionally – amount to unfair treatment of competitors. Google, for instance, has been found to prioritise its own products and services over those of competitors when ranking search results.[8] Such anti-competitive practices are not uncommon. The European Commission and EU member states levied more than €20 billion in fines on Big Tech companies for anti-competitive practices between 2016 and 2019 (Scott and Larger 2019). When used for pricing purposes, software can also lead to collusive market outcomes, either purposefully (facilitation of explicit collusion) or as an unintended emergent result (tacit collusion) (Ezrachi and Stucke 2016, OECD 2017, CMA 2018).

Equality law. Software is increasingly used in the context of making decisions that affect individuals, be it in the private sector (e.g. algorithms used to inform hiring decisions, determine credit eligibility, or provide targeted pricing) or in the public sector (e.g. algorithms to inform policing practices, determine the allocation of health resources, identify children at risk of harm, or predict households likely to enter into fuel poverty). In such cases, the way in which the software is programmed can come into conflict with equality law requirements, including the avoidance of unlawful discrimination and, when it comes to software use in the public sector, the Public Sector Equality Duty.

Data protection law. Digital ways of collecting, curating, processing, sharing, and storing personal data invariably involve a variety of software solutions. Some of these solutions may have weaknesses that raise questions related to compliance with data protection legislation. Software can also be at play in the deliberate flouting of data protection requirements. For example, there is evidence to suggest that companies use cookies to track individuals' online habits and share that information with multiple advertising partners around the world in ways that violate the provisions of the European Union's General Data Protection Regulation (e.g. Libert 2015, ICO 2019, Murgia and Harlow 2019).

8 See the 2017 case by the European Commission against Google (https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784).

Product safety. The details of a given piece of software can be relevant from the perspective of product safety regulation, be it through software being embedded in physical products or software tools constituting products in their own right. In either case, software can be the cause of product safety violations. Software-related product safety issues can arise in any sector. We give two examples here to illustrate the forms that such issues can take:

- *Transport.* Software plays an increasingly important role in the operation of motor vehicles such as cars and lorries, passenger airplanes and trains, commercial ships, as well as the transport infrastructure itself. This includes the use of software to operate specific parts (e.g. a vehicle's brakes) or to automate the operation of entire systems (e.g. automated trains or driverless cars). As manufacturers increasingly rely on software to control devices, errors in the code or in the design of the code are bound to arise. In the most extreme cases, such as the two plane crashes caused by poorly designed flight control software aboard Boeing's 737 Max, software can lead to devastating loss of life.
- *Health.* Software is also increasingly used in the medical field. This includes software that is embedded in machines (e.g. the Therac-25 radiation therapy machine), used as part of operations (e.g. to triage patients in A&E), or deployed to support diagnostic decisions (e.g. as a software tool for reading X-rays or analysing CT scans). When used in any of these situations, inadequate code can harm or even threaten the lives of patients.

Integrity and stability of financial markets. In the financial sector, software is used in applications that can have implications for market integrity and financial stability. For example, software used for financial trading may have features that – intentionally or unintentionally – result in trading patterns that amount to insider trading or illicit forms of market manipulation. Similarly, trading software or software used for risk management can produce destabilising market dynamics (e.g. flash crashes) or the violation of capital requirements, either through errors or as a result of purposeful programming.

Environmental protection. In cases where source code is embedded within products with a regulated environmental impact, such as automobiles, software features may be relevant to questions of compliance with the relevant requirements. For example, software tweaks were used to manipulate the results of emissions tests by several car manufacturers.[9]

Gambling regulations. Software-related issues have been around for decades in the gambling industry. In the 1990s, for example, Ronald Harris, a software engineer for Nevada's Gaming Control Board, inserted fraudulent code into more than 30 slot machines. The code would trick the slot machines into triggering jackpots when users

9 In the past, many large automobile manufacturers have been fined for cheating on emissions tests by manipulating technology in their cars, including Volkswagen (in 2015), Fiat Chrysler Automobiles (2017), General Motors (2015), and Daimler (2019).

inserted coins in a specific order (Koeppel 2006). Although this is an example of a rogue employee intentionally inserting malicious code into a small number of slot machines, concerns related to more systemic use of software to rig gambling machines or applications abound.

Consumer protection. Several reports outline the challenges of consumer protection in the digital age (e.g. OECD 2019). As software is embedded in more and more products and services that we use in our lives and homes, it gives rise to concerns related to privacy, security, hidden deficiencies or aftermarket support. A well-known example of the interplay between consumer protection laws and software embedded in physical devices relates to Apple's iOS updates for iPhones. Towards the end of 2017, it became increasingly clear that the updates that Apple was pushing for iPhones limited the battery performance of older iPhone models. There have been multiple class-action lawsuits against Apple, accusing it of undermining the performance of its older products in order to encourage customers to purchase newer phones. The lawsuits against Apple are likely to be only the tip of the iceberg when it comes to software that might come in conflict with consumer protection law.

As these examples show, needs for source code analysis for regulatory or judicial purposes can arise in many different contexts. For each of the examples above, conclusive assessments of compliance and lawfulness may not be possible without access to source code or may be easier and cheaper to achieve by accessing the underlying code.

Governments and their agencies may require access to source code either before a product or service containing software enters the market or after it was sold and problems appeared. The first situation can be thought of as a need for *ex-ante* disclosure of source code – accessing source code for conformity assessments and regulatory approvals. These assessments and approvals can be a precondition for the sale, distribution, or use of certain types of software. The second situation can be thought of as a need for *ex-post* disclosure of source code – accessing source code as part of investigations, enforcement activities, and legal proceedings in response to incidents or suspected violations of regulatory or legal requirements. We discuss *ex-ante* and *ex-pos*t disclosure in greater detail below.

3.1.1 Ex-ante disclosure for regulatory purposes

Requirements of ex-ante regulatory approval or independent conformity assessments for certain types of products, services, projects, or processes are a well-established practice in many jurisdictions. Medical devices and vehicles, for example, commonly need to undergo independent assessments and obtain regulatory approval before being admitted to the market. Depending on the context, such assessments and approvals may be carried out by regulatory authorities themselves or may rely on delegation, for example in the form of certification schemes administered by accredited organisations.

Software may become subject to ex-ante regulatory approvals or conformity assessment requirements in one of two ways. First, software may be part of products, services or processes that are themselves subject to regulatory approvals or conformity requirements (e.g. cars, medical devices, or voting machines). Second, software can be a standalone product or tool that, in its own right, is subject to regulatory approvals or assessment requirements – for example, in the case of a software tool for interpreting CT scans or a model used by a financial institution to calculate capital requirements.

Insofar as regulatory approvals or conformity requirements touch on software features, there can be cases in which an adequate analysis of the software involved may be difficult or impossible to achieve without access to source code. At the time of writing, regulatory approval and conformity assessment procedures rarely involve the analysis of source code. However, the vehicle emissions scandals mentioned above or recent controversies about voting machines[10] provide vivid evidence of the limitations of this approach and illustrate why governments may decide to introduce requirements for source code disclosure to regulatory authorities or other entities conducting conformity assessments.

Beyond these present-day examples, the growing adoption of machine learning is set to increase the role of software disclosure in regulatory approval and conformity assessment procedures. Technical capabilities enabled by machine learning will lead to the introduction of software-based solutions in domains and sectors in which software has played a less prominent role in the past. Whether used in new or established areas, machine learning will contribute to software becoming increasingly complex.

The complexity of software based on machine learning approaches can make it harder to manage risks and can also lend itself to the concealment of the intentional violation of regulatory and legal requirements. Both of these factors are potential reasons for the introduction of regulatory approval and conformity assessment requirements in areas where such requirements have not existed in the past. Increases in software complexity can also mean that there is a growing need to analyse the software's source code in order to arrive at sufficiently conclusive results for regulatory approval and conformity assessment purposes: performance tests, the review of software specifications, and other assessment approaches that do not require source code access can be less conclusive as the complexity of software systems increases.

10 The software used in Dominion voting machines in the 2020 US presidential election was blamed incorrectly by Donald Trump for mistakes in vote counts coming from the states of Michigan and Georgia (Nicas 2020). Although the software was not deemed to be at fault in the end, important questions were raised about certifying voting machines and ensuring trust in the electoral process. Prior to the 2020 election, researchers uncovered vulnerabilities in online voting systems and apps. For example, Specter et al. (2020) conducted research on a mobile voting app used in the 2018 midterm elections in West Virginia, US which had vulnerabilities that made it possible to alter, stop, or expose a user's vote; Halderman and Teague (2015) conducted research related to an internet voting system used in the 2015 state election in New South Wales, Australia which had vulnerabilities that could be exploited to change votes, identify voters, or bypass the verification mechanism.

Recent years have seen a rapidly growing debate about regulatory questions that arise in the context of machine learning systems. Requirements for technology providers or users to participate in certification schemes or otherwise seek regulatory approval play a prominent role in these debates. While it is too early to judge their outcome, it is easily conceivable that these debates will lead to novel regulatory approval and conformity assessment requirements; and that some of those requirements will involve ex-ante disclosures of source code.

Countries are increasingly looking at regulatory solutions to ensure that software innovation based on machine learning approaches is responsible and safe. In the US, the Commodity Futures Trading Commission has contemplated rules that would require financial institutions to make source code used for high frequency trading generally accessible to the regulator.[11] Similarly, regulators in the UK are increasingly devoting resources to understanding how to regulate software based on machine learning approaches. Ambitious agendas and strong calls for greater transparency have been set out by the Information Commissioner's Office in publications such as *Explaining decisions made with Artificial Intelligence*[12] and *Guidance on AI and Data Protection*;[13] the Competition and Markets Authority in *Algorithms: How they can reduce competition and harm consumers*;[14] and Ofcom in *Regulating video-sharing platforms*.[15] Publications from other regulators will soon follow. The Financial Conduct Authority, for example, is collaborating with The Alan Turing Institute on a report regarding AI transparency in financial services. The Equality and Human Rights Commission are also working alongside The Alan Turing Institute and the Centre for Data Ethics and Innovation to produce guidance on compliance with the Equality Act 2010 when using complex software solutions.

In the UK, regulation of technologies based on machine learning is dynamic, fast moving, and ambitious. The UK has a tremendous opportunity to lead the global conversation on the regulation of these powerful technologies. As software-based technologies, part of that conversation will inevitably be around the need for ex-ante source code disclosure.

3.1.2 Ex-post disclosure for regulatory and judicial purposes

Setting aside the need for ex-ante source code disclosure as part of regulatory approvals or conformity assessments, source code disclosure may also be needed to enable authorities to determine relevant facts in response to incidents, suspected violations of regulatory and legal requirements, or other disputes involving software. As with ex-ante disclosure, access to source code will not always be necessary to determine the facts in question, but

11 In the end, these rules were not adopted.
12 https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence/
13 https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/
14 www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers
15 www.ofcom.org.uk/__data/assets/pdf_file/0021/205167/regulating-vsp-guide.pdf

in some cases the relevant facts are difficult or impossible to establish without access to source code. The likelihood of this being the case will increase with the adoption of more complex software solutions.

Relevant facts that may need to be determined include questions of compliance and lawfulness across virtually all domains, as the examples at the beginning of this section illustrated. Such questions may arise in the context of investigations and enforcement activities carried out by regulatory bodies or in the context of legal proceedings. For example, source code analysis may be needed to determine whether:

- a given piece of software contributed to anti-competitive outcomes and whether it was deliberately programmed to do so;
- the use of a given decision-making algorithm is inconsistent with equality law requirements;
- personal data is processed and shared in ways that violate data protection law;
- accidents are attributable to failures to conform to product safety requirements;
- a financial trading algorithm is designed to pursue strategies that amount to unlawful market manipulation.

When it comes to legal proceedings, disputes may also concern facts that go beyond compliance and lawfulness. These include, for instance, questions such as determining whether an accident caused by a partly automated vehicle or some other software-reliant product is due, say, to a manufacturing defect or to inappropriate use. Source code can also be key evidence in intellectual property infringement cases.

In contrast to ex-ante source code disclosure requirements, which are relatively rare in the existing regulatory and legal landscape, ex-post disclosure requirements have clearly established precedents in many jurisdictions. Often, such requirements will have a basis in general regulatory or legal powers. It is worth noting, however, that there are also examples of dedicated legal provisions that give authorities specific powers to request the disclosure of source code in certain contexts. In the US, for example, the Internal Revenue Code explicitly provides for the possibility of authorities requesting access to the source code of tax software where they cannot otherwise reasonably ascertain the accuracy of an item on a return.[16]

Ex-post source code disclosure requirements can involve making the relevant code accessible to the appropriate regulatory, administrative, or judicial authorities or to other organisations or individuals involved in carrying out the needed assessments. The analysis of source code by independent experts played an important role, for example,

16 26 U.S. Code §7612 - Special procedures for summonses for computer software.

in Toyota's unintended acceleration lawsuits. *Bookout and Schwarz v. Toyota* is a case brought against the car manufacturer following a 2007 car accident that led to the death of the passenger and the serious injury of the driver. Faulty software caused the car to continue accelerating despite the driver's attempts to engage the hand and foot brakes. NASA was initially tasked with examining the source code of the software embedded in the 2005 Toyota Camri involved in the crash. NASA software engineers found 7,134 violations when they checked Toyota's source code against MISRA-C, a coding standard for software embedded in cars. Michael Barr, a software specialist, and Phillip Koopman, a professor in Electrical and Computer Engineering at Carnegie Mellon University, were subsequently tasked with reviewing Toyota's source code further. Their review uncovered 81,514 violations against the coding standard. Barr and Koopman's testimonies proved pivotal, convincing the jury not only of the fact that Toyota's software was defective, but also that the company acted in "reckless disregard of the rights" of the plaintiffs (Safety Research & Strategies 2013). Cases like this underline the importance of technical specialists and academic researchers having access to source code in order to determine relevant facts in response to incidents, suspected violations of regulatory and legal requirements, or other disputes involving software.

3.2 Meeting procurement needs

Government-mandated source code disclosure requirements can also serve the purpose of meeting information needs that arise in procurement contexts. When organisations procure software or software-driven products and services, the ability to access the software's source code can matter for a variety of objectives, including due diligence, transparency and accountability, or strategic aims. In light of the potential dependence of these objectives on source code accessibility, governments may decide to enact rules that require procurement contracts to include source code accessibility conditions or that provide a legal basis (where needed)[17] for procuring entities to give preference to contracts that include such conditions.

The most salient procurement context in which government-mandated source code disclosure requirements may exist relates to procuring goods and services for the public sector. Across jurisdictions, it is common practice for governments to set specific rules for public procurement. Such rules often require public bodies only to enter into – or to give preferential treatment to – procurement contracts that include certain conditions. When it comes to procurement that involves software, these conditions may touch on source code. In particular, conditions might include the sharing of the software's source code with the procuring public sector body and other government entities for purposes

17 For example, in the context of public sector procurement where such preferential treatment could otherwise be open to legal challenge.

of scrutiny; granting licences to share the source code publicly; or a more comprehensive assignment of intellectual property rights in the software and its source code to the procuring body.

Such conditions can be implemented through bespoke contractual provisions. Alternatively, they can be achieved through adherence to independently established default arrangements. A particularly prominent example of the latter approach relates to requirements or preferential treatment for technology that is provided on the basis of open source licences, which allow software to be freely used, modified, and shared.[18]

The UK government made a commitment in 2016 to have source code be open by default.[19] This commitment is reflected in the *Government Design Principles*,[20] where the 10th principle states:

> "We should share what we're doing whenever we can. With colleagues, with users, with the world. Share code, share designs, share ideas, share intentions, share failures."

The government's *Technology Code of Practice*[21] echoes that advice ("publish your code and use open source software to improve transparency, flexibility and accountability"), as do the recently published *Guidelines for AI procurement*[22] ("ensure your work is open and available to others for reuse"). Such commitments – and extensive guidance – highlight the relevance of open source licensing arrangements to recent public procurement policy debates.

When it comes to possible motivations for public procurement rules that require or give preference to contracts that allow source code access, the following purposes can be distinguished.

3.2.1 Due diligence

Access to source code can enable procuring bodies to perform their own assessment of a given piece of technology at a level that is sufficiently detailed for due diligence purposes. Relevant dimensions of assessment include questions of regulatory compliance and lawfulness across the various areas outlined at the beginning of this section, including requirements that apply specifically to the public sector, such as the Public Sector Equality Duty. They also include broader aspects of fitness for purpose, safety, and trustworthiness, which are important to any responsible procurement process and essential for procurement processes in the public sector.

18 https://opensource.org/osd
19 www.gov.uk/government/publications/open-source-guidance
20 www.gov.uk/guidance/government-design-principles
21 www.gov.uk/government/publications/technology-code-of-practice/
22 www.gov.uk/government/publications/guidelines-for-ai-procurement/guidelines-for-ai-procurement

One context with elevated requirements of scrutiny is the procurement of technology that is considered *critical national infrastructure*, with examples ranging from communication network equipment to technology used in elections.[23] Recent controversies about the use of Huawei kit in 5G networks in the US and the UK and allegations of election irregularities in the US have highlighted the particularly pronounced need to ensure the trustworthiness of software involved in operating such critical national infrastructure. Other contexts include technology that has national security implications, such as software used in the defence sector, and situations that involve the deployment of software within protected digital environments, which exist in many areas of the public sector. For example, software is sometimes built to analyse valuable, sensitive, or highly personal data which may be held in protected environments. The ability to scrutinise source code is essential to ensuring that the software used within these protected environments does not compromise data security.

When it comes to due diligence, open source licensing arrangements have a key advantage in that they entail the ability to publish source code, which means that it can be scrutinised by a wider audience, outside of the procuring entity. As the *Government Design Principles*[24] state when advocating for open source software, "the more eyes there are on a service the better it gets – howlers are spotted, better alternatives are pointed out, the bar is raised". Due diligence processes are enhanced as a result of making source code widely available.

3.2.2 Transparency and accountability

The accessibility of source code for software procured by public sector bodies can also be important in order to meet demands of transparency and accountability concerning the use of a given piece of software. Relevant demands can take two forms. First, beyond the need to ensure that software is compliant, fit for purpose, safe, and trustworthy, software users will often face a need to *demonstrate publicly* that the software used has these properties. Second, in cases where software is used for decision-making purposes, there can be a need to explain and justify these decisions (ICO 2020).

While these two types of needs are not limited to the use of software by public sector bodies, they can be particularly pronounced in this context, in part due to legal reasons. And both needs can have implications for the accessibility of source code that may go beyond those associated with due diligence needs. More specifically, public demonstrations of safety and trustworthiness may include making source code publicly available, regardless of whether there is a case for the publication of source code from a due diligence perspective; and an organisation's ability to explain and justify software-based decisions may require the analysis of source code even if such analysis is not deemed necessary for due diligence purposes.

23 www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical
24 www.gov.uk/guidance/government-design-principles

3.2.3 Strategic considerations

Finally, source code accessibility requirements can be rooted in strategic considerations faced by organisations procuring technology that go beyond the purposes of due diligence or transparency and accountability. In particular, open source licensing arrangements or other contractual provisions that enable the procuring entity to modify, re-purpose, or share source code can have significant financial and technological benefits.

From a financial perspective, such arrangements can significantly reduce the cost of updating or improving a given piece of software by allowing for these activities to be carried out in-house or based on open tendering. It can also make it possible to re-deploy a given software tool in new contexts without additional cost. These benefits are particularly salient for the public sector, where value-for-money considerations play a prominent role in procurement processes.

In terms of technological benefits, such arrangements can reduce the likelihood of organisations being tied into particular types of operating infrastructure for the use of a given software tool. The public sector has a long history of procurement contracts that result in government departments and agencies being locked into long-term relationships with software providers. Source code accessibility requirements can help mitigate these long-standing issues.

***

In the UK, the procurement of software in the public sector is subject to numerous policies and extensive guidance. As software-based technologies evolve, these policies and guidelines are also changing and placing greater emphasis on the need for transparency. Recent documents such as the government's *Guidelines for AI procurement*[25] provide horizontal guidance for software solutions that rely on machine learning, while documents such as *A buyer's guide to AI in Health and Care*[26] provide sector-specific guidance. The need for transparency is underlined in all recent guidelines related to the public procurement of software-based products and services.

While our discussion here focuses on source code accessibility provisions in public-sector procurement rules, it is worth noting that governments may in principle also issue rules where such provisions apply to private-sector procurement practices. In particular, in response to due diligence and transparency/accountability needs, governments may decide to enact measures designed to require or prioritise source code accessibility for certain types of technology procurement in the private sector.

25 Available at www.gov.uk/government/publications/guidelines-for-ai-procurement/guidelines-for-ai-procurement
26 www.nhsx.nhs.uk/ai-lab/explore-all-resources/adopt-ai/a-buyers-guide-to-ai-in-health-and-care/

3.3 Promoting innovation and economic development

Finally, governments may introduce source code disclosure requirements that are intended to promote innovation and economic development. The availability of source code developed by a technology provider to other organisations can be an impactful mechanism to accelerate technology adoption, spur new inventions, ensure interoperability between technology solutions, and foster the growth of a country's industrial ecosystem.

Source code disclosure requirements motivated by these considerations can take various forms. They may involve source code being made available publicly or to specific organisations, with or without the permission to use or modify it. Relevant examples include, once again, measures that require or incentivise arrangements that make source code available on an open source basis, for example through rules for procurement contracts in the public sector or elsewhere. Another prominent example with particular relevance to trade agreements are measures specifically dedicated to technology transfer at the international level. For instance, governments may enact investment rules that require foreign technology developers investing in a given country to form joint ventures with domestic companies, entailing domestic ownership of the intellectual property for imported technology (e.g. through provisions in investment treaties). Considerations of technology transfer can be particularly relevant in the context of developing economies, with the possibility of trade agreement provisions including exceptions for countries depending on their level of economic development. Considerations of international technology transfer can also be relevant in other contexts, however. For example, governments may seek to require or encourage the transfer of technologies that are deemed essential to the mitigation of emergencies or crises.

4 SOURCE CODE DISCLOSURE IN RECENT TRADE AGREEMENTS

Trade agreements and negotiations have taken notice of the important role of source code in international commerce. As a result, several recent agreements have specific provisions related to source code disclosure. In this section, we introduce the legal mechanisms for protecting source code and note that the limitations of these mechanisms are pushing countries to introduce provisions related to source code disclosure in bilateral trade agreements. We then examine the provisions related to source code disclosure in seven recent trade agreements, highlighting some of their differences and limitations. We end the section by analysing the enforcement mechanisms in each of the seven agreements we examined.

4.1 Legal mechanisms for protecting source code

The legal mechanism that is most widely used to protect source code is trade secret law. Trade secrets, however, are not the only type of IP protection available to software creators. The expression of a programmer's ideas in source code can be protected through copyright law, for example, and truly innovative software can be protected through patents.

Yet, these alternative protections leave gaps. Copyright law, for example, protects the specific way in which a piece of code is written, but not the more general idea of how the software functions. Patent protections are limited in time, and often not available for all parts of a software-based system.[27] Machine learning approaches, for instance, might not be patentable where they are considered too abstract.[28] Moreover, patent applications generally require disclosure of the innovation in question, which might make the information disclosed ineligible for trade secret protection.[29] The limitations of copyright law, combined with the cost and uncertainty of patenting software, have meant that software producers and innovators rely mostly on trade secret protection rather than other IP protections available.

Article 39 of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) offers protection for trade secrets.[30] The software code disclosure provisions included in recent bilateral agreements, however, go further than Article 39 of TRIPS. In particular – and of interest to us in this chapter – the provisions place limitations on the power of public authorities to mandate access to source code.

4.2 Provisions related to source code disclosure in recent trade agreements

In this section, we examine the source code disclosure provisions in the following agreements:[31]

- the US–Japan Digital Trade Agreement (US–Japan) (2019)[32]
- the United States–Mexico–Canada Agreement (USMCA) (2018)[33]
- the EU–Japan Economic Partnership Agreement (EU–Japan) (2018)[34]
- the EU–UK Trade and Cooperation Agreement (EU–UK) (2020)[35]
- the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (2018)[36]

27 *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014)
28 Article 52, European Patent Convention, and Guidelines for Examination by the European Patent Office (www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm).
29 Despite transparency requirements seemingly putting patents and trade secrets at odds, there are legal avenues for innovators to maintain the secrecy of their inventions during the process of patent applications (e.g. McGurk and Lu 2015).
30 www.wto.org/english/docs_e/legal_e/27-trips.pdf
31 We selected these agreements based on (1) the wide coverage they provide of negotiating parties and their respective interests; and (2) the fact that they allow us to see how provisions have evolved over time. The years in parentheses represent the year when each agreement was signed.
32 https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf
33 https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between
34 https://trade.ec.europa.eu/doclib/press/index.cfm?id=1684
35 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948119/EU-UK_Trade_and_Cooperation_Agreement_24.12.2020.pdf
36 www.dfat.gov.au/sites/default/files/tpp-11-treaty-text.pdf; to be read in conjunction with the text of the Trans-Pacific Partnership (TPP) (www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents).

- the Indonesia–Australia Comprehensive Economic Partnership Agreement (IA-CEPA) (2020)[37]
- the Japan–Mongolia Economic Partnership Agreement (Japan-Mongolia) (2015).[38]

The agreements above establish a general prohibition on public authorities requiring the transfer of, or access to, source code of software owned by a person of the other Party (also referred to as source code disclosure in this document). The prohibition aims to encourage trade by banning source code disclosure mandates as a condition for market access.

The agreements allow for a number of exceptions. A holistic reading of each agreement is necessary to develop a full picture of the exceptions that relate to the source code provision. First, the articles related to source code in each agreement contain some safeguarding exceptions. Second, each agreement includes exceptions that apply to the scope of the treaty's various provisions taken together which, by implication, also apply to the provisions contained in the article on source code disclosure. Both types of exceptions provide potential bases for the parties to the agreements to require the disclosure of source code under certain conditions. Typically, the burden of proof to show that a given disclosure requirement is justified pursuant to one of the exceptions falls on the party that is enacting the requirement.

The exceptions in the trade agreements that we examined build on earlier exceptions in WTO agreements. Some of the agreements we looked at incorporate the well-known Articles XX GATT 1994 & Article XIV GATS (general exceptions for public interest measures) or Article XXI GATT & Article XIV bis GATS (national security exception). In general, these provisions provide a basis for justifying government conduct that goes against general treaty obligations, including the general prohibition on source code disclosure requirements, by requiring that:

1. the government conduct pursues a legitimate public interest;
2. the measures taken are either necessary or relevant to the achievement of this public interest (depending on the provision);
3. the measures implemented in order to pursue the goal do not constitute arbitrary or unjustifiable discrimination or a disguised restriction on international trade.

Table 1 provides a summary of the legitimate public goals that the trade agreements we examined recognise as justifying government measures that diverge from treaty provisions.[39] Since the focus of this chapter is source code disclosure, the table concentrates

37 www.dfat.gov.au/trade/agreements/in-force/iacepa/iacepa-text/Pages/default
38 www.mofa.go.jp/files/000067716.pdf
39 The exact wording of the articles in each trade agreement that specifically refer to source code is available in the Appendix.

on the legitimate public purposes that are explicitly mentioned in the agreements and that have a clear relationship to the disclosure of source code embedded in software services or products using software.

TABLE 1 EXPLICITLY STATED EXCEPTIONS TO THE GENERAL PROHIBITION ON SOURCE CODE DISCLOSURE REQUIREMENTS[40]

	US-Japan[1]	USMCA[2]	EU-Japan[3]	EU-UK[4]	CPTPP[5]	IA-CEPA[6]	Japan-Mongolia[7]
Disclosure to a public or judicial authority during specific targeted investigations, inspections, or proceedings	X*	X*		X			
General disclosure requirements necessary to secure compliance with/ enforcement of laws or regulations, explicitly including:	X[8]	X[9]	X	X	X**	X**	X[10]
Competition law enforcement			X	X			
IP protection and enforcement			X	X[11]	X*	X*	X[12]
Tax law and customs law enforcement	X[13]	X[14]	X	X[15]			X[16]
Prevention of deceptive practices or deal with effects of default	X[17]	X[18]	X[19]	X[20]			X[21]
Privacy and data protection	X[22]	X[23]	X[24]	X[25]			X[26]
Safety	X[27]	X[28]	X[29]	X*			X[30]
Protect public morals, order or safety	X[31]	X[32]	X[33]	X[34]			X[35]
Protect human, animal or plant life or health	X[36]	X[37]	X[38]	X[39]			X[40]
Financial system integrity and stability	X[41]	X[42]***	X[43]	X[44]			

40 An in-depth reading of the text of each of these treaties, as well as other relevant documents, may be necessary to provide greater clarity on whether the treaties can be interpreted in a manner to justify source code disclosure in a particular case. Another preliminary note to make is the fact that financial and investment services are treated separately from electronic commerce in many of these agreements. The row on 'financial stability and integrity' includes a mark (X) only where there is an explicit exception to the general prohibition on source code disclosure for the purpose of financial stability and integrity. Footnotes allow the reader to consult the original source in the legal texts. Unless otherwise indicated through footnotes, the relevant provisions can be found in the articles referred to in the top row of the table.

	US-Japan[1]	USMCA[2]	EU-Japan[3]	EU-UK[4]	CPTPP[5]	IA-CEPA[6]	Japan-Mongolia[7]
Limit prohibition of source code disclosure requirements to mass market software or products using such software and excluding critical infrastructure					X	X	X
Government procurement		X[45]	X[46]	X[47]	X[48]	X[49]	
Essential security interests / national security	X[50]	X[51]	X[52]	X[53]		X	X[54]
Reassurance disclosure does not relate to proprietary or confidential information held, collected, processed by public authorities		X[55]	X[56]****	X[57]****	X[58]		
Commercially negotiated contracts			X	X	X	X	
Voluntary transfer of source code			X	X			

Notes: * Subject to appropriate safeguards to prevent unauthorised disclosure of source code. ** Requiring modification of source code for the purposes of compliance with the law rather than requiring source code disclosure. *** Only restrictive measures related to payments or transfers are included in this exception. **** No disclosure of information that is contrary to the essential security interests of a party to the agreement can be mandated. [1] Article 17, US-Japan. [2] Article 19.16, USMCA. [3] Article 8.73, EU-Japan, referring to Article III Government Procurement Agreement and Articles 1.5, 8.3 and 8.65 of EU-Japan. [4] Article DIGIT.12, EU-UK, referring to Article DIGIT.4 of EU-UK and Article III Government Procurement Agreement as incorporated by Article PPROC.2 of EU-UK. [5] Article 1, CTPP referring to Article 14.17, Trans-Pacific Partnership Agreement. [6] Article 13.13, IA-CEPA. [7] Article 9.11, Japan-Mongolia. [8] Article 3, US-Japan, referring to Article XIV GATS. [9] Article 32.1.2, USMCA, referring to Article XIV GATS. [10] Article 1.10.1, Japan-Mongolia, referring to Article XIV GATS and Article XX GATT. [11] Article DIGIT.12, EU-UK. In the context of public procurement, Article PPROC.2 of EU-UK referring to ANNEX PPROC-1 of EU-UK, Section A, referring to Article III Government Procurement Agreement. [12] Article 1.10.1, Japan-Mongolia, referring to Article XX(d) GATT, reinforced by Article 12.1.1, Japan-Mongolia. [13] Article 3, US-Japan, referring to Article XIV GATS. [14] Article 32.1.2, USMCA, referring to Article XIV GATS. [15] Article EXC.1.1, EU-UK, referring to Article XX GATT. [16] Article 1.10.1, Japan-Mongolia, referring to Article XIV GATS and Article XX GATT. [17] Article 3, US-Japan, referring to Article XIV GATS. [18] Article 32.1.2, USMCA, referring to Article XIV GATS. [19] Article 8.3.2(c)(i), EU-Japan. [20] Article EXC.1.1, EU-UK, referring to Article XX GATT; Article EXC.1.2.(c)(i), EU-UK. [21] Article 1.10.1, Japan-Mongolia, referring to Article XIV GATS and Article XX GATT. [22] Article 3, US-Japan, referring to Article XIV GATS. [23] Article 32.1.2, USMCA, referring to Article XIV GATS. [24] Article 8.3.2(c)(ii), EU-Japan. [25] Article EXC.1.2(c)(ii), EU-UK. [26] Article 1.10.1, Japan-Mongolia, referring to Article XIV GATS. [27] Article 3, US-Japan, referring to Article XIV GATS. [28] Article 32.1.2, USMCA, referring to Article XIV GATS. [29] Article 8.3.2(c)(iii), EU-Japan. [30] Article 1.10.1, Japan-Mongolia, referring to Article XIV GATS. [31] Article 3, US-Japan, referring to Article XIV GATS. [32] Article 32.1.2, USMCA, referring to Article XIV GATS. [33] Article 8.73, EU-Japan, but also Article 8.1.2 of EU-Japan, Article 8.3.2(a) and Article 8.3.1 of EU-Japan referring to Article XX GATT; Article 8.73.2(c) of EU-Japan referring to Article III Government Procurement Agreement. [34] Article EXC.1.1, EU-UK, referring to Article XX GATT; Article EXC.1.2(a) of EU-UK; Article EXC.1.2.(c)(iii) of EU-UK; In the context of public procurement – Article PPROC.2 of EU-UK referring to ANNEX PPROC-1 of EU-UK, Section A, referring to Article III Government Procurement Agreement. [35] Article 1.10.1, Japan-Mongolia, referring to Article XIV GATS and Article XX GATT. [36] Article 3, US-Japan, referring to Article XIV GATS. [37] Article 32.1.2, USMCA, referring to Article XIV GATS. [38] Article 8.3.2(b), EU-Japan; Article 8.73.2(c) of EU-Japan referring to Article III GPA. [39] Article EXC.1.1, EU-UK, referring to Article XX GATT; Article EXC.1.2(b) of EU-UK; in the context of public procurement - Article PPROC.2 of EU-UK referring to ANNEX PPROC-1 of EU-UK, Section A, referring to Article III Government Procurement Agreement. [40] Article 1.10.1, Japan-Mongolia, referring to Article XIV GATS and Article XX GATT. [41] Article 5, US-Japan. [42] Article 32.4, USMCA. [43] Article 8.65, EU-Japan. [44] Article SERVIN 5.39, EU-UK. [45] Article 19.2.3(a), USMCA. [46] Article 8.73.1, EU-Japan, but also Article 8.73.2(c) of EU-Japan referring to Article III Government Procurement Agreement. [47] A set of justifications (incorporated into the table), found in Article PPROC.2 of EU-UK referring to ANNEX PPROC-1 of EU-UK, Section A, referring to Article III Government Procurement Agreement. [48] Article 1, CPTPP, referring to Article 14.2, Trans-Pacific Partnership Agreement. [49] Article 13.2.3, IA-CEPA. [50] Article 4(b), US-Japan. [51] Article 32.2.1, USMCA. [52] Article 8.73.2(c), EU-Japan, referring to Article III Government Procurement Agreement. [53] Article EXC.4(b)(i), EU-UK; Article PPROC.2 of EU-UK referring to ANNEX PPROC-1 of EU-UK, Section A, referring to Article III Government Procurement Agreement. [54] Article 1.10.1, Japan-Mongolia, referring to Article XIV bis GATS. [55] Article 19.2.3 (b), USMCA, with the exception of provisions relating to open government data. [56] Article 1.5.1(a), EU-Japan. [57] Article EXC.4(a), EU-UK. [58] Article 13.2.4, IA-CEPA.

As the table illustrates, the agreements we examined exhibit significant overlap in terms of their explicitly mentioned potential justifications for allowing governments and their agencies to require access to source code. They have a tendency to converge around similar sets of commonly accepted public interests, values, or circumstances that justify the disclosure of source code. At the same time, there are notable conceptual differences. For example, there is a shared recognition that source code disclosure may be required to ensure compliance and enforcement of laws, but differences when it comes to the particular legal or public interests explicitly recognised by individual agreements. There are also differences in terms of requirements to balance disclosure interests against other interests under the exceptions that agreements provide for – for example, the above-mentioned requirements (2) and (3) set out in Articles XIV GATS or Article XX GATT to demonstrate necessity or relevance and for measures to take forms that do not constitute arbitrary discrimination or a disguised restriction on international trade.

The exceptions contained in individual agreements resonate, to different degrees, with the range of possible reasons for government-mandated source code disclosure requirements discussed in Section 3. For example, source code disclosure for the purpose of compliance with or enforcement of laws and regulations is enshrined in many of the trade agreements we examined. Similarly, the agreements often exempt government procurement from the scope of the general prohibition on requiring source code disclosure and carve out some exceptions for the disclosure of source code in the interest of governmental interests such as the protection of national security or critical infrastructure.

In many agreements, however, the exceptions to the general prohibition on requiring access to source code are comparatively narrow, and none of the agreements that we examined covers all of the scenarios outlined in Section 3. While this finding might not come as a surprise – carving out exceptions for all relevant scenarios is not trivial – we find it worrisome that the exceptions in some agreements cover very few of the scenarios outlined in Section 3. Building future-proof provisions for the disclosure of source code in trade agreements is a challenging task. The starting point, however, must be what we know about software-based technologies today and the various scenarios that they give rise to, as outlined in Section 3. We recommend that trade negotiators give thorough consideration to all of these scenarios in formulating exceptions to general prohibitions on requiring access to source code.

For the rest of this section, we outline consequential differences in the wording of the articles relating to source code, as they appear in the agreements that we examined. Where relevant, we also provide recommendations for future negotiations.

4.2.1 The challenge of defining regulatory and judicial needs

The Japan–Mongolia Economic Partnership Agreement was the first to include an article related to source code. The article itself, 9.11, only included a single exception: it noted that "for the purposes of this Article, software [...] is limited to mass-market software or products containing such software, and does not include software used for critical infrastructure".

The agreements that followed the Japan–Mongolia Economic Partnership Agreement expanded the list of exceptions incorporated into the articles related to source code. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership added wording to specify that Article 14.17, which relates to source code, "shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes". The EU–Japan Economic Partnership Agreement went much further, broadening the list of exceptions included in Article 8.73, which refers to source code, to competition law, intellectual property rights, essential security interests, and other legitimate public interests.

The fast-changing nature of software-based services and products – along with their widespread impacts on societies and economies – make it impossible to draft a complete and future-proof list of all areas of compliance and lawfulness where source code disclosure may be needed. Recognising this difficulty, the United States–Mexico–Canada Agreement and the US–Japan Digital Trade Agreement took a different approach from their predecessors. The two agreements note that their respective articles related to source code (19.16 in USMCA and 17 in US–Japan) do not "preclude a regulatory body or judicial authority of a Party from requiring a person of the other Party to preserve and make available the source code of software [...] for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure". This language provides a partial solution to the issue of having to enumerate all possible situations when source code disclosure might be required for regulatory and judicial needs.

The approach taken in Article 19.16 of USMCA and Article 17 of US–Japan is a promising way of getting around the challenging task of enumerating all possible situations when source code disclosure might be required. Should similar approaches become the norm in future trade agreements, we recommend that the wording in the source code articles allows for a wider range of actors to require access to source code. Organisations other than regulatory bodies or judicial authorities might have an interest in accessing source code, for example, for the purpose of conformity assessments.

4.2.2 Protection of source code vs. algorithms

The articles related to source code in the agreements that we examined establish a general prohibition on public authorities requiring "the transfer of, or access to, source code of software". The United States–Mexico–Canada Agreement and the US–Japan Digital Trade Agreement are, once again, notable exceptions here, as they extend the

general prohibition on disclosure requirements to algorithms. In particular, Article 19.16 in USMCA and Article 17 in US–Japan ban mandatory transfers and access to "the source code of software [...] or an algorithm expressed in that source code".

As we saw in Section 2, algorithms are pieces of code that contain a series of steps that need to be followed in order to solve a computational problem. As such, the lines of code that specify how an algorithm functions are covered under the general prohibition on requiring "the transfer of, or access to, source code of software". It is unclear what additional protections, besides the lines of code themselves, the wording in Article 19.16 of the USMCA and Article 17 in US–Japan provides to algorithms. However, the existence of that wording opens the door to arguing for protections whose scope extends beyond the lines of code themselves and include, for example, more high-level descriptions of the operating logic of a given piece of software.

If the exceptions that an agreement provides for are unduly narrow, this kind of expanded scope of the general prohibition on disclosure requirements can aggravate the resulting implications in problematic ways. While often insufficient to develop a reliable understanding of a given piece of software, the analysis of general descriptions of algorithmic logic can be helpful in partly addressing the needs identified in Section 3. Compared to provisions that only preclude the accessibility of source code to meet such needs, provisions that additionally also preclude the accessibility of general descriptions of software logic should therefore be interpreted as entailing more severe undue constraints. Given the difficulties of ensuring that the exceptions specified in a proposed agreement are sufficiently comprehensive and future-proof, negotiators should exercise caution in expanding the scope of the general prohibition to include algorithms.

4.2.3 Access to versus modification of source code to secure compliance with the law

The safeguarding exceptions incorporated within the articles related to source code are generally couched in terms of *access* to source code. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership and the Indonesia–Australia Comprehensive Economic Partnership Agreement are the only agreements among the ones that we examined to diverge from this. To secure compliance with law and regulations, the CPTPP and IA–CEPA agreements provide for the possibility to require the *modification* of source code but not to require access to it. This severely limits the ability of national authorities to ensure compliance with or enforcement of laws and regulations. In future trade negotiations, we strongly recommend against the approach taken by the CPTPP and IA–CEPA agreements. The possibility of requiring access to source code must be secured for the purpose of compliance with or enforcement of laws and regulations.

4.2.4 Voluntary or commercially negotiated transfer of source code

Among the agreements we examined, two of them explicitly state that voluntary source code disclosure is unaffected by the general prohibition (the EU–Japan Economic Partnership Agreement and the EU–UK Trade and Cooperation Agreement). Four of the agreements we examined explicitly acknowledge that the general prohibition does not affect source

code disclosure as a result of commercially negotiated contracts. Yet, although the other trade agreements do not explicitly mention the voluntary or commercially negotiated transfer of source code, this does not mean that they prohibit such transfers.

The legal principle of freedom of contract, in particular, allows private parties to agree on the terms and conditions of their interaction in a legally enforceable document as long as they do not contradict existing laws. The trade agreements that do not explicitly recognise voluntary or commercially negotiated source code disclosure do not prohibit such conduct. However, the agreements that explicitly acknowledge the legality of voluntary or commercially negotiated source code disclosure provide an additional layer of transparency and clarity in this regard. We recommend that future trade agreements provide this clarity, especially for voluntary source code disclosure. Such clarity may be particularly valuable in encouraging practices like open source or open and reproducible science.

4.3 Enforceability of provisions relevant to source code disclosure

Enforcement is a key consideration when it comes to trade agreements. Without effective enforcement mechanisms in place, countries might not have an incentive to abide by the rights and obligations stipulated in international legal texts.

International trade disputes take place between legally equal sovereigns – be it nation states or trade blocs with a jurisdiction over certain territories. Because of this, dispute settlement procedures often include a diplomatic process of mutual consultation before any legally binding dispute settlement proceedings commence. This seeks to provide a forum for the parties to reach a mutually agreeable solution. The WTO Dispute Settlement Understanding similarly provides for this diplomatic step of consultation between the parties before turning to the Dispute Settlement Body for a binding decision.[41] In some trade agreements, parties are also invited to explore alternative methods of dispute resolution, such as good offices, conciliation, or mediation, although there is no obligation to do so.[42] This manner of dispute settlement – inviting parties to consultation and exploring alternative dispute resolution methods before establishing panels or tribunals – reflects the steps in the WTO's Dispute Settlement Understanding.[43]

If the parties do not reach a mutually agreed solution through consultations, they can request the establishment of a panel or arbitration tribunal, created for the purposes of the particular trade dispute. These dispute settlement tribunals or panels conclude their work with a decision or a report which is binding on the parties of the agreement.

41 Article 4, Dispute Settlement Understanding.
42 See, for example, Article 31.5 of USMCA.
43 For an overview of the process of the typical WTO dispute settlement, see https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c6s1p1_e.htm.

Obligations spelled out in trade agreements range from requiring the responding party to "whenever possible, eliminate the non-conformity"[44] to taking "the necessary measures to comply immediately with the ruling".[45]

States are subject to multiple trade agreements. Many of the agreements that we examined account for this fact. They recognise that an action by a state can be an alleged breach of more than one trade agreement to which that state is a party. In such circumstances, the agreements provide for the possibility of countries choosing which dispute settlement forum to use in order to address their grievance. This highlights that there may be more than one pathway for requesting an impartial decision on matters of compliance with the text of the trade agreements.

With the exception of the US–Japan Digital Trade Agreement, all of the agreements we examined include agreement-specific enforcement mechanisms. In the case of the US–Japan Digital Trade Agreement, there are still potential avenues for seeking to resolve disputes between the parties through appeal to an independent authority. Notably, the International Court of Justice (ICJ), within the United Nations system, is available to adjudicate on disputes between any states party to its Statute which willingly submit a case to it. According to Article 93(1) of the Charter of the United Nations, all UN member states are ipso facto parties to the Statute. Cases before the ICJ can fall within the scope of any international treaty,[46] which would include trade agreements such as these discussed in this chapter.

Table 2 summarises the procedural steps of the dispute settlement procedures in the trade agreements we examined. As the table illustrates, all but one of the trade agreements we examined provide for meaningful pathways to independent assessment and enforcement of rights and obligations arising out of the agreements. In all cases where there is a dispute resolution mechanism detailed in the agreement itself, the source code non-disclosure provision and relevant exceptions fall within the scope of this mechanism. Where no such mechanism is provided by the agreement, general fora like the International Court of Justice remain available to the parties to uphold the treaties.

44 Article 28.19.2 of TPP Agreement.
45 Article INST.21.1 of EU-UK Trade and Cooperation Agreement.
46 Articles 34-36, Statute of the International Court of Justice.

TABLE 2 DISPUTE SETTLEMENT PROCESSES RELEVANT TO THE GENERAL PROHIBITION OF REQUIRING SOURCE CODE DISCLOSURE AND RELEVANT EXCEPTIONS

	US-Japan	USMCA[1]	EU-Japan[2]	EU-UK[3]	CPTPP[4]	IA-CEPA[5]	Japan-Mongolia[6]
Parties must have good faith consultations prior to legally binding dispute settlement proceedings		X[7]	X[8]	X[9]	X[10]	X[11]	X[12]
Parties can choose alternative dispute resolution methods, like good offices, conciliation, mediation		X[13]	X[14]		X[15]	X[16]	X[17]
Parties can choose the dispute settlement forum if the subject matter is a breach of multiple agreements that both states are a party to		X[18]	X[19]	X[20]	X[21]	X[22]	X[23]
Binding decision by an ad hoc arbitration tribunal or panel		X[24]*	X[25]*	X[26]*	X[27]*	X[28]	X[29]
Complaining Party is allowed to suspend treaty obligations proportionately in case of the Responding Party's non-compliance with decision		X[30]	X[31]	X[32]	X[33]	X[34]	x[35]
No formal dispute resolution mechanism specified	X						

Notes: * Arbitrators or panellists are to be chosen from a pre-agreed list of qualified individuals. Some agreements provide for an exception where no qualified individuals are on the lists. [1] Chapter 31, USMCA. [2] Chapter 21, EU-Japan. [3] Article INST.10 on the scope of the Dispute settlement mechanism under EU-UK. [4] Chapter 28, TPP. [5] Chapter 20, IA-CEPA. [6] Chapter 16, Japan-Mongolia. [7] Article 31.4, USMCA. [8] Article 21.5, EU-Japan. [9] Article INST.13.1, EU-UK. [10] Article 28.5, TPP. [11] Article 20.5, IA-CEPA. [12] Articles 16.2 and 16.4, Japan-Mongolia. [13] Article 31.5, USMCA and Article 31.22, USMCA. [14] Article 21.6, EU-Japan. [15] Article 28.6, TPP. [16] Article 20.6, IA-CEPA. [17] Article 16.5, Japan-Mongolia. [18] Article 31.3, USMCA. [19] Article 21.27, EU-Japan. [20] Article INST.12.1, EU-UK. [21] Article 28.4, TPP. [22] Article 20.4, IA-CEPA. [23] Article 16.3, Japan-Mongolia. [24] Article 31.6, USMCA, on the establishment of a panel and Article 31.8, USMCA, on the pre-agreed roster of panelists to choose from. Article 31.9.3, USMCA, on the possibility to exceptionally nominate a panelist who is not from the roster. Articles 31.18, USMCA, on the impact of the panel's report. [25] Article 21.7 and Article 21.9, EU-Japan, on pre-established list of arbitrators; Article 21.15.8, EU-Japan, on the binding nature of the decision of the panel; Article 21.20, EU-Japan, on compliance with the final report of the panel. [26] Articles INST.14 and INST.15, EU-UK, on the establishment of the arbitration tribunal; Articles INST.27 and INST.28, EU-UK, on the pre-agreed arbitrators to choose from; Article INST.29.1, EU-UK, on the binding nature of tribunal decisions. [27] Article 28.7, TPP, on establishing the panel; Article 28.11, TPP, on the roster of panelists; Article 28.19, TPP, on the binding nature of the panel report. [28] Article 20.8, IA-CEPA, on establishing the panel; Article 20.12.1, IA-CEPA, on the binding nature of the panel's findings. [29] Article 16.6, Japan-Mongolia, on establishing an arbitration tribunal; Article 16.11.1, Japan-Mongolia, on the requirement to comply with the arbitral decision. [30] Article 31.19, USMCA. [31] Article 21.22, EU-Japan. [32] Article INST.24, EU-UK. [33] Article 28.20, TPP. [34] Article 20.14, IA-CEPA. [35] Article 16.11.4, Japan-Mongolia.

5 CONCLUSION

Software-driven technologies, made all the more powerful by machine learning approaches, have become a transformative social, political, and economic force. As they continue to improve and grow, they give rise to unprecedented opportunities but also to novel challenges for policymakers.

Trade negotiators, in particular, face the difficult task of establishing provisions that balance a multitude of competing interests, ranging from commercial interests, to national economic and security interests, and to the fundamental rights and freedoms of individuals. Compared to other issues covered by trade agreements, finding the right balance between these interests when it comes to the treatment of source code disclosure is particularly challenging. This is because of the rapidly evolving and partly unpredictable nature of software-based innovation, its increased importance in international commerce, and the multitude of reasons why governments and their agencies might require access to source code.

This chapter provides a primer on the issue of source code disclosure in the context of trade negotiations. We covered what source code is, the main programming approaches, and the crucial role of humans when things go wrong. We outlined the possible motivations for government-mandated source code disclosure requirements and the forms that such requirements can take. Finally, we examined how a number of recent trade agreements address the issue of source code disclosure, identifying along the way some consequential differences in the wording of articles relating to source code.

Despite the ground that we covered here, more work remains to be done. We focused on the question of when disclosure of source code may be needed. How the disclosure needs are best translated into legal text as well as how the disclosure itself should be managed in practice will require additional research and deliberation. Furthermore, in this chapter we primarily questioned whether the current provisions related to source code can be improved. We did not, however, ask the important question of whether a general prohibition on requiring the transfer of, and access to, source code is the best way to handle the protection of software innovations in trade agreements. Further research is needed to ascertain that this is the best path to take. Finally, looming large over any trade agreement are questions related to the economic impact of the provisions. At the time of writing, no research exists on the effect that provisions related to source code disclosure have on international trade.

Software is not only here to stay, but will play an ever-bigger role in our lives and businesses. Trade agreements are only one area where the fine balance between enabling innovation and mitigating risks needs to be found. In finding that balance, UK trade negotiators must ensure that trade agreements complement the country's ambitious regulatory and economic agenda in pursuit of responsible software-based innovation.

APPENDIX: ARTICLES FROM INTERNATIONAL TRADE AGREEMENTS RELATING TO SOURCE CODE

US-Japan Digital Trade Agreement

Article 17: Source code

1. Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of the other Party to preserve and make available[47] the source code of software, or an algorithm expressed in that source code, for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.

United States-Mexico-Canada Agreement

Article 19.16: Source code

1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding,[48] subject to safeguards against unauthorized disclosure.

47 This making available shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner.

48 This disclosure shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner.

EU-Japan Economic Partnership Agreement

Article 8.73: Source code

1. A Party may not require the transfer of, or access to, source code of software owned by a person of the other Party.[49] Nothing in this paragraph shall prevent the inclusion or implementation of terms and conditions related to the transfer of or granting of access to source code in commercially negotiated contracts, or the voluntary transfer of or granting of access to source code for instance in the context of government procurement.
2. Nothing in this Article shall affect:
   a. requirements by a court, administrative tribunal or competition authority to remedy a violation of competition law;
   b. requirements by a court, administrative tribunal or administrative authority with respect to the protection and enforcement of intellectual property rights to the extent that source codes are protected by those rights; and
   c. the right of a Party to take measures in accordance with Article III of the GPA.
3. For greater certainty, nothing in this Article shall prevent a Party from adopting or maintaining measures[50] which are inconsistent with paragraph 1, in accordance with Articles 1.5[51], 8.3[52] and 8.65[53].

EU-UK Trade and Cooperation Agreement

Article DIGIT.12: Transfer of or access to source code

1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party.
2. For greater certainty:
   a. the general exceptions, security exceptions and prudential carve-out referred to in Article DIGIT.4 [Exceptions] apply to measures of a Party adopted or maintained in the context of a certification procedure; and
   b. paragraph 1 of this Article does not apply to the voluntary transfer of, or granting of access to, source code on a commercial basis by a natural or legal person of the other Party, such as in the context of a public procurement transaction or a freely negotiated contract.

49 For greater certainty, "source code of software owned by a person of the other Party" includes source code of software contained in a product.
50 Those measures include measures to ensure security and safety, for instance in the context of a certification procedure.
51 Security exceptions
52 General exceptions
53 Prudential carve-out

3. Nothing in this Article shall affect:

    a. a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a Party's competition law to prevent or remedy a restriction or a distortion of competition;
    b. a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online, subject to safeguards against unauthorised disclosure;
    c. the protection and enforcement of intellectual property rights; and
    d. the right of a Party to take measures in accordance with Article III of the GPA as incorporated by Article PPROC.2 [Incorporation of certain provisions of the GPA and covered procurement] of Title VI [Public procurement] of this Heading.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership

Article 14.17: Source code

1. No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.

2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.

3. Nothing in this Article shall preclude:

    a. the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or
    b. a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.

4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.

Indonesia-Australia Comprehensive Economic Partnership Agreement

Article 13.13: Source code

1. Neither Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.

2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure, or software that is specifically made for use by a Party.

3. Nothing in this Article shall preclude:

   a. the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or
   b. a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.

4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.

5. Nothing in this Article shall prevent a Party from adopting or maintaining any measures that it considers necessary for the protection of its essential security interests.

Japan-Mongolia Economic Partnership Agreement

Article 9.11: Source code

1. Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, as a condition of the import, distribution, sale or use of such software, or of products containing such software, in its Area.

2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software, and does not include software used for critical infrastructure.

REFERENCES

CMA – Competition and Markets Authority (2018), "Pricing algorithms: Economic working paper on the use of algorithms to facilitate collusion and personalised pricing", 8 October (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf).

CMA (2021), "Algorithms: How they can reduce competition and harm consumers", 19 January (www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers).

Coughlan, S (2021), "A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco", BBC, 26 August (www.bbc.com/news/education-53923279).

Desai, D and J A Kroll (2018), "Trust but verify: A guide to algorithms and the law", *Harvard Journal of Law and Technology* 31(1).

Ezrachi, A and M E Stucke (2016), *Virtual Competition*, Harvard University Press.

Guglya, L and M Maciel (2016), "Addressing the digital divide in e-commerce JSI: From enabling issues to data and source code provisions", CUTS International (www.cuts-geneva.org/pdf/200615-E-Commerce-Issue_Paper.pdf).

Halderman, J A and V Teague (2015), "The New South Wales iVote system: Security failures and verification flaws in a live online election", *International Conference on e-Voting and Identity,* Springer, pp. 35–53.

ICO – Information Commissioner's Office (2019), "Update report into adtech and real time bidding", 20 June (https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf).

ICO (2020), "Explaining decisions made with AI", 20 May (https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/).

Koeppel, D (2006), "Casino hackers", CNN, 23 October (https://edition.cnn.com/2006/TECH/07/13/popsci.gambling/).

Leslie, D (2020), *Understanding bias in facial recognition technologies: An explainer*, The Alan Turing Institute (https://doi.org/10.5281/zenodo.4050457).

Leslie, D, L Holmes, C Hitrova and E Ott (2020), *Ethics of machine learning in children's social care*, What Works for Children's Social Care (https://whatworks-csc.org.uk/wp-content/uploads/WWCSC_Ethics_of_Machine_Learning_in_CSC_Jan2020.pdf).

Leveson, N G and C S Turner (1993), "An investigation of the Therac-25 accidents", *Computer* 26(7): 18–41.

Libert, T (2015), "Privacy implications of health information seeking on the web", *Communications of the ACM* 58(3): 68–77.

McCann, D (2019), *e-Commerce free trade agreements, digital chapters and the impact on labour: A comparative analysis of treaty texts and their potential practical implications*, New Economics Foundation (www.ituc-csi.org/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf).

McGurk, M R and J W Lu (2015), "The intersection of patents and trade secrets", *Hastings Science and Technology Law Journal* 7: 189.

Murgia, M and M Harlow (2019), "How top health websites are sharing sensitive data with advertisers", *Financial Times,* 13 November (www.ft.com/content/ofbf4d8e-022b-11ea-be59-e49b2a136b8d).

Nicas, J (2020), "No, Dominion voting machines did not delete Trump votes", New York Times, 11 November (www.nytimes.com/2020/11/11/technology/no-dominion-voting-machines-did-not-delete-trump-votes.html).

OECD – Organisation for Economic Co-operation and Development (2017), *Algorithms and collusion: Competition policy in the digital age* (www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf).

OECD (2019), *Challenges to consumer policy in the digital age* (www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf).

Office for National Statistics (2020), "Annual gross fixed capital formation by industry and asset" (www.ons.gov.uk/file?uri=/economy/grossdomesticproductgdp/datasets/annualgrossfixedcapitalformationbyindustryandasset/current/bb20anngffindassetfinalqa.xls).

Safety Research & Strategies (2013), "Toyota unintended acceleration and the big bowl of 'spaghetti' code", 7 November (www.safetyresearch.net/blog/articles/toyota-unintended-acceleration-and-big-bowl-%E2%80%9Cspaghetti%E2%80%9D-code).

Schwartz, O (2019), "In 2016, Microsoft's racist chatbot revealed the dangers of online conversation", IEEE Spectrum, 25 November (https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation).

Scott, M and T Larger (2019), "To take on big tech, US can learn antitrust lessons from Europe", Politico.eu, 31 August (www.politico.eu/article/europe-us-big-tech-competition-antitrust-apple-google-facebook-amazon/).

Specter, M A, J Koppel and D Weitzner (2020), "The ballot is busted before the blockchain: A security analysis of Voatz, the first internet voting application used in US federal elections", *29th USENIX Security Symposium*, pp. 1535 – 1553.

Wu, M (2017), "Digital trade-related provisions in regional trade agreements: Existing models and lessons for the multilateral trade system", RTA Exchange, International Centre for Trade and Sustainable Development and Inter-American Development Bank.

ABOUT THE AUTHORS

Cosmina Dorobantu is the Deputy Director of The Alan Turing Institute's public policy research programme. She is a member of the Financial Conduct Authority and the Bank of England's Artificial Intelligence Public-Private Forum, as well as the Trade and Economy Panel within the UK's Department for International Trade. She holds a PhD in Economics from the University of Oxford and is a Research Associate at the University's Oxford Internet Institute.

Florian Ostmann is the Policy Theme Lead within The Alan Turing Institute's public policy programme. He is a member of the Royal Statistical Society's Data Science Section Committee and the Law Committee for the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. He holds a PhD in Political Philosophy from University College London and a Master's degree in Public Policy from Harvard Kennedy School.

Christina Hitrova is a doctoral candidate with the Professorship for Law, Science and Technology at the Technical University of Munich. Christina spent two years at The Alan Turing Institute, researching AI ethics. She was also a trainee with the European Commission's Legal Service, working within the Trade policy and WTO team. Christina holds Master's degrees in Law from KU Leuven and the University of Zurich.

CHAPTER 5

The difficult past and troubled future of digital protectionism

Susan Ariel Aaronson
George Washington University and CIGI

OVERVIEW

America's former Commerce Secretary Wilbur Ross did not mince words. In a 2018 *Financial Times* op-ed, he argued that the lack of clarity around Europe's data protection rules, the General Data Protection Regulation (GDPR), could hamper information-sharing between governments and businesses across the Atlantic, and that in turn would impede trade.[1] Ross was implying that the European Union's effort to protect personal data before it could flow between nations was 'protectionist'.

However, Ross's assertion was a bit unfair. Most agreements designed to govern cross-border data flows include provisions designed to protect personal information and the privacy of users (Monteiro and Teh 2017: 51-53, Casolini and Lopez-Gonzalez 2019: 16, 27, Lopez-Gonzalez and Ferencz 2018). Moreover, most trade agreements – including the most internationally accepted agreement, the WTO – include exceptions which allow signatories to breach the agreement's rules in the interest of protecting privacy, public health, public morals, national security, or intellectual property,[2] as long as such restrictions are necessary, proportionate, and do not discriminate among signatories (Monteiro and Teh 2017: 23-24).

Although Ross is no longer in government, Europeans and Americans still struggle to find common ground on how best to govern data at the national and international levels.[3] Policymakers in Europe, Canada[4] and other countries are considering, or have established, rules to enhance data sovereignty and digital sovereignty, two related concepts. *Data sovereignty* can be defined as the notion that various types of data have a home country and should be governed by that home country's (or region's) rules when stored in the cloud. *Digital sovereignty* relates to ownership and control of the infrastructure where data is

1 https://thehill.com/policy/technology/389948-wilbur-ross-says-gdpr-could-hurt-trade
2 General Agreement on Trade in Services (GATS), "Marrakesh Agreement Establishing the World Trade Organization", Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, 15 April 1994 (www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm).
3 https://fortune.com/2020/07/16/cjeu-kills-privacy-shield-facebook-schrems and www.cpomagazine.com/data-protection/a-tangled-twisted-route-to-privacy-shield-invalidity/
4 www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html.

stored. On 29 October 2019, German Chancellor Angela Merkel announced that the EU should reclaim its 'digital sovereignty' by developing its own platform to manage data and reduce its reliance on US data-driven firms (Chazen 2019). The German government explained that digital sovereignty is "the possibility of independent self-determination by the state and by organizations with regard to the use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result."[5]

Europe has taken several steps to ensure data and digital sovereignty. It is creating a European cloud designed to facilitate Europe's digital sovereignty. The EU has also drafted a data strategy, building on its commitment to protecting personal data as well as the desire to encourage various sectors of society to share and mix data.[6] According to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, "with the General Data Protection Regulation, Europe asserts its digital sovereignty and gets ready for the digital age…The new rules are beginning to set a global standard for privacy. They will help to bring back the trust we need to be successful in a global digital economy."[7]

The transatlantic divide over whether privacy is protectionism or whether the EU can achieve sovereignty over data and data infrastructure provides a perfect illustration of the muddied debate over what is or is not digital protectionism. In this chapter, I examine the past and troubled future of digital protectionism. I argue that the future is troubled because policymakers have not adequately focused on the broad panoply of barriers, including those that affect trust and internet stability (such as censorship or disinformation).

I begin by defining digital protectionism, a term which is constantly evolving as data-driven services and data governance evolve. While digital protectionism can refer to barriers to digitally delivered goods and services, the analysis herein focuses on barriers to cross-border data flows. Next I discuss what trade agreements actually say about barriers to cross-border data flows. I note that most digital trade agreements include language governing performance requirements for source code or server location rules, but do not address other potential trade barriers such as internet shutdowns, DDOS attacks, disinformation, or censorship. These barriers make it harder for users and thwart a trusted environment for digital trade. I then briefly examine three of these potential barriers in depth and discuss whether they are likely to be addressed in future trade agreements or trade disputes. I conclude with some suggestions for policymakers.

5 www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6, 3.

6 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, a European strategy for data", COM(2020) 66 final, 19 February 2020 (https://digital-strategy.ec.europa.eu/en/policies/strategy-data).

7 "Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation," European Commission, 24 May 2018 (https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889).

THE PROBLEM IS IN THE NATURE OF DATA: THE DEFINITION OF DIGITAL PROTECTIONISM

The OECD notes that there is no one internationally accepted definition for digital trade. However, "there is a growing consensus that it encompasses digitally-enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments."[8] Not surprisingly, there is also no internationally shared definition for digital protectionism. Policymakers in many nations are just beginning to define what they see as barriers and what they view as legitimate regulations for data, data-driven services, and digital trade (Casolini and Lopez-Gonzalez 2019, Lopez-Gonzalez and Ferencz 2018, Aaronson and Struett 2020) . In 2018, the US Trade Representative defined digital protectionism as laws and regulations that block the flow of data across borders, impede the provision of services such as cloud computing, or otherwise restrict the ability of firms to take advantage of best-in-class digital services.[9] For the purposes of analysis herein, I focus only on barriers (alleged and those covered in trade agreements) to cross-border data flows and not to digital trade per se, as illustrated in Box 1.

Because the internet is a shared platform built on cross-border data flows, ideally nations would work to ensure digital market openness. The OECD defines digital market openness as the ability of foreign suppliers to compete in national markets without encountering discriminatory, excessively burdensome or restrictive conditions. But policymakers must also create an enabling environment (i.e. laws and regulations) that allow "digital transformation to flourish" (López González and Ferencz 2018: 34). Not surprisingly, nations have different visions of how best to encourage such digital transformation. Moreover, digitalisation may simultaneously be altering the terms of competition, blurring the boundaries of markets, and changing our understanding of how regulations affect trade (López González and Ferencz 2018: 34). Other studies report similar findings (Macedoni and Weinberger 2019).

8 www.oecd.org/trade/topics/digital-trade/

9 "Key Barriers to Digital Trade", USTR Fact Sheet, March 2018 (https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital). In 2020, it did not define these barriers (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)

BOX 1 BARRIERS TO CROSS-BORDER DATA FLOWS

Discriminatory treatment

- Foreign investment restrictions
- Intermediary liability without safe harbor or fair-use provisions
- 'Snippet tax' on search engines that quote text snippets as part of search results
- Taxes on over-the-top (OTT) services such as media, messaging, or VOIP
- Web filtering and blocking of content and other forms of censorship

Localisation barriers

- Data localisation and server localisation requirements
- Limited or no access to foreign government procurement markets
- Requirement for use of local technology
- Comprehensive privacy regulations that may discriminate against foreign providers

Technology barriers

- Restrictions or prohibitions on use of encryption
- Source code, technology, or other intellectual property rights (IPR) forced transfer requirements
- Local testing and certification for imported information technology (IT) equipment

Other barriers

- Cybersecurity threats or local requirements
- Weak IPR enforcement
- Restrictions to online advertising
- Surveillance
- DDOS attacks
- Disinformation

Sources: Aaronson (2018a); Casolini and Lopez-Gonzalez (2019); Fefer (2019); Ferencz (2019).

Digital protectionism is not well understood. Scholars do not know which barriers are the most trade-distorting and even whether digital protectionism is growing or remaining stable. However, digital protectionism does seem increasingly visible (Chander and Le 2014, 2015, Aaronson 2018a, Corey 2018, 2019). There are several reasons why.

1. The nature of data

Digital protectionism differs from traditional protectionism because trade in data is different from trade in goods and other services. Data is intangible and highly tradeable, and some types of data, when processed, are a public good, which governments must provide and regulate effectively (Aaronson: 2018b). In contrast with physical goods, 'netizens' can trade that same digital good simultaneously. Moreover, trade in digital services differs from trade in other services because suppliers and consumers do not need to be in the same physical location for a transaction to occur. Given these attributes, it may be hard for researchers to ascertain exactly what a government wants to protect and whether a government is acting with protectionist intent.

2. Data as a trade problem

Data crosses borders constantly, and location is hard to determine on a borderless network. Trade in the same set of data can occur repeatedly in nanoseconds (e.g. when millions of people download Drake's latest song). Researchers and policymakers may find it hard to determine what is an import or export. They also struggle to ascertain when data is subject to domestic law (such as IP law) and what type of trans-border enforcement is appropriate (Goldman 2011, de la Chapelle and Fehlinger 2016). Policymakers cannot easily determine jurisdiction, because data can be routed through a US server to another jurisdiction. Consequently, data flows may travel through several countries before reaching their destination (de la Chapelle and Fehlinger 2016).

3. Data governance is a work in progress

Data governance is an essential component of good governance in the 21st century and will have important effects on economic as well as human rights outcomes, such as freedom of speech, access to information, and privacy. Researchers have shown that as data-driven technologies become more widespread, the governance of data becomes more important (Belton 2019). Moreover, given its political and economic importance, the failure to influence governance of data could undermine trust in governance, democratic values, and in the internet as a whole.

But in high-, medium- and low-income countries alike, policymakers struggle to keep pace with data-driven change. No one knows what comprehensive and effective data governance looks like at the national and international levels. According to the UNCTAD cyberlaw tracker, while 82% of countries in 2020 have e-transaction laws, only 56% of countries have consumer protection laws, only 66% have personal data protection laws,

and only 80% have cyber-crime laws.[10] Moreover, having these laws does not mean a country has the capacity, funds or will to effectively utilise and enforce them. Finally, tomorrow's internet and uses for data may require new laws and regulations, such as regulations to ban certain types of AI (e.g. facial recognition), discriminatory effects from using certain types of predictive analytics or behavioural targeting, and so on.

4. No clear dividing line between legitimate and trade-distorting governance

There is no roadmap or clear paradigm that policymakers can utilise to distinguish between legitimate domestic regulation for data, platforms, and e-commerce and trade-distorting data flow regulation. From late 2018 to March 2019, the Global Digital Protectionism project surveyed experts from business, government, academia, and civil society who worked on trade, data, or internet governance issues. We did not seek to obtain a representative sample, but rather to better understand the diversity of views about how these people saw data governance and the barriers to cross-border data flows. We found a lack of consensus on definitions, how and when policymakers can block trade flows under current trade agreements under the exceptions, and how best to respond to digital trade barriers. We also did not find agreement on whether policymakers should ban certain practices (such as censorship) or rely on the exceptions to preserve domestic data governance policy space.[11]

5. Data governance is normative, yet everyone would benefit from a shared approach to data governance that promotes trust and interoperability

Many allegations of digital protectionism reflect concerns about different approaches to regulating the data flows that underpin the internet within national borders. We see this in former Secretary Ross's assertion that personal data protection is protectionist, while EU officials argue that privacy and personal data must be adequately protected before data can flow across borders. Some scholars argue that while concerns about surveillance, privacy, and security are legitimate, they may transform the internet into the 'splinternet' (Chander and Le 2014, 2015, Aaronson and LeBlond 2018) . Yet, instead of making interoperability of data governance regimes a priority, some nations – in particular, the US, the EU and China – are pushing the world to accept their paradigms for digital trade and data governance (Aaronson and Leblond 2018, Buchser and Hakmeh 2019). Meanwhile, to their credit, Australia and Singapore in their Digital Economy Agreement[12] and Chile, Singapore and New Zealand in their Digital Economy Partnership Agreement[13] have made fostering trust in cross-border data flows a top priority (Aaronson and Struett 2020).

10 https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide

11 See www.digitaltradepolicy.org/ and, for an overview of survey findings, https://b45b15ec-a610-4874-8e79-455a81822ca0.filesusr.com/ugd/4c8157_92a733637c5d40d9ab6346d60623905e.pdf

12 www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement

13 www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement

6. The data and development dilemma

The future of the digital economy is in the developing world, yet many developing countries lack digital prowess and data norms and rules. Without such prowess, national policymakers may not yet be comfortable governing data. Analysts have found that several low- and-middle-income nations such as India and Indonesia have growing digital prowess. However, no low-income developing nation has significant digital prowess as of this writing, nor are any major exporters of data-driven services. These nations lack infrastructure as well as expertise – they have lower levels of connectivity, limited digital expertise, national technological, financial and logistical challenges, and weaker regulatory and institutional frameworks (UNCTAD 2020: para. 14). Moreover, these countries do not have large numbers of constituents demanding that policymakers develop rules to govern data.

Political scientist Steven Weber noted that many developing countries may, over time, fail to develop a data-driven economy and therefore be forced into a data trade imbalance (Weber 2017: 412-413). International organisations such as UNCTAD and the World Bank have recognised this dilemma and suggested that policymakers need to deepen their understanding of trade, digitalisation and governance (World Bank 2016, UNCTAD 2017). These nations will likely need help to better understand how to use data to facilitate development — a very different approach from the traditional route of graduating from exporting commodities and then moving exports from manufactures to services (Aaronson 2019). Developing countries could be at risk of becoming "mere providers of raw data to global digital platforms, based mainly in the United States and China, while having to pay such platforms for the digital intelligence produced from their data" (UNCTAD 2020: para. 41).

7. Digital protectionism could yield negative spillovers

To reiterate, policymakers may have good reasons to limit the free flow of data across borders. However, when states restrict the free flow of data, they reduce access to information, which in turn can diminish economic growth, productivity, and innovation both directly and globally (Maskus and Reichman 2004, OECD 2016). In so doing, states may also reduce internet stability and generativity. Over time, increased intervention could lead to more legal disputes, higher costs, and ultimately a splintered internet (Daigle 2015, Drake et al. 2016, López González and Ferencz 2018).

CURRENT MODELS FOR DIGITAL TRADE AND WHAT THEY SAY ABOUT DIGITAL PROTECTIONISM

Policymakers have been negotiating bilateral e-commerce and digital trade agreements since the early days of the 21st century,[14] but until recently these agreements said little explicitly about digital protectionism.

Much of the language in digital trade chapters or agreements was highly influenced by the US approach to governing the internet, regulating the companies that provide its infrastructure, and regulating the various types of data that underpin that network of networks (Aaronson 2015). The United States began that effort in 1997 when then President Clinton announced a Framework for Global Electronic Commerce. This framework articulated what the regulatory environment "should" look like if nations wanted to encourage national and global e-commerce. The Framework focused on private sector leadership, a limited role for government intervention, and principles to reassure consumers that their data would be protected and secure.[15]

But to some extent the effort to build trust in e-commerce by ensuring netizens that they and their data would be safe took a back seat to the notion of free flow of data across borders. Free flow of data would allow US companies to expand their access to data and better serve their clients (advertisers) and users. The Clinton administration made clear that "the US government supports the broadest possible free flow of information across international borders". This Framework very much influenced the OECD Action Plan for Electronic Commerce, which in turn influenced the bilateral and regional agreements on e-commerce described below (Aaronson 2015; Aaronson 2018b). However, I will show that this current approach is insufficient to address even the current barriers.

1. Free flow as the default and the broad use of the exceptions

Almost every recent agreement has binding language like "neither 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."[16] But policymakers also acknowledge that nations have other important policy objectives such as preserving public order, privacy, consumer welfare, or public morals. Hence nations can meet these obligations by using an exception as justification.[17] These agreements

14 Australia and Singapore signed the first digital trade agreements with commitments on the free flow of data across borders for service suppliers and investors (www.dfat.gov.au/sites/default/files/safta-third-review-outcomes-at-a-glance.pdf).

15 https://clintonwhitehouse4.archives.gov/WH/New/Commerce/

16 US-Japan, Article 11 (https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf and ARticle 4.2); DEPA, Articles 4.2 and 4.3 (www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf).

17 The exceptions include measures necessary to (a) protect public morals or to maintain public order; (b) protect human, animal or plant life or health; (c) secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts; (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; and safety (www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf).

generally incorporate both the GATT (Articles XX and XXI) and GATS exceptions (Articles XIV).[18] All of these trade agreements also include a national security exception, which allows signatories to breach the rules to protect against what its policymakers see as a national security threat. Nations using these exceptions do not have to justify their use to other nations.[19] However, when nations use the exceptions, they must be necessary and be designed to be as least trade-restrictive as possible.[20]

Nations are supposed to turn to these exceptions only in extraordinary circumstances. However, there are few shared norms and definitions regarding how nations should behave when rules governing data flows conflict with the achievement of other important policy objectives (Aaronson 2018a, 2018b). Therefore, these exceptions risk becoming the rule without the further development of mechanisms to bridge regulatory differences between countries (World Economic Forum 2019). For example, the US argued that it needed to ban foreign suppliers of internet gambling to protect public morals (Burri 2013) and, more recently, argued that it needed to ban Chinese apps TikTok and WeChat for national security reasons (Aaronson 2020). When nations rely on the exceptions, other nations could challenge them in a trade dispute, although it may be in all nations' interests to keep the exceptions vague.

Moreover, some argue that the exceptions were not built for the digital age. Economist Daniel Ciuriak argues that socially harmful use of data such as 'fake news' and disinformation in personally targeted advertising and/or messaging (for example, for exploitation of psychological vulnerabilities for marketing purposes or for political manipulation) should also be considered a legitimate exception (Ciuriak 2019).

2. Different approaches to personal data protection and privacy

Trade policymakers have long recognised that protecting the privacy and personal data of their citizens is an important aspect of good governance. As noted earlier, most trade agreements delineate that nations can breach free flow of data rules to protect privacy (Monteiro and Teh 2017).

But nations have adopted different approaches. The US, New Zealand, and Canadian FTAs generally state that the Parties agree that because consumer and personal data protection are important, signatories should enforce their own laws, which in turn should be built on

18 For example, "Nothing in this Agreement shall be construed to:(a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests".

19 "Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or(b)preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests", DEPA, Article 15.2 (www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf).

20 They use language like "such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail".

international principles such as the APEC Privacy Framework or the OECD Guidelines.[21] The Parties also recognise the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.

Meanwhile, the human rights of EU citizens cannot be addressed in trade agreements because privacy and personal data protection are fundamental rights under the EU Constitution. Thus, the EU requires evidence and a formal determination that personal data will be sufficiently protected before it can flow across borders. Signatories to EU digital trade agreements must first be deemed adequate for personal data to flow freely to and from those nations and the EU. However, as of March 2021, only 14 nations are deemed 'adequate'.[22] Not surprisingly, as of this writing, the EU has fewer binding digital trade agreements or chapters [23] than other nations such as Australia or Canada (Monteiro and Teh 2017, Fefer 2019, Aaronson and Struett 2020).

Moreover, because the EU insists on the extraterritorial application of its rules to other nations, its approach could be seen as bullying. For example, the UK left the EU in 2020 and UK Digital Minister Dowden suggested that the UK might make some changes to its approach to personal data protection. In March 2021, EU Justice Minister Reynders warned that "[i]f problematic divergences take place, that will trigger the suspension or withdrawal clause of our adequacy decision".[24]

Several digital trade templates have aspirational language encouraging nations to build their data protection regimes on widely accepted principles such as those put forward by APEC and the OECD. The 2020 Australia–Singapore Digital Economy Agreement seems to be the first agreement calling for interoperability of data protection regimes. Interoperability would make data protection more effective, as national approaches would be more coherent at the international level. It notes that "each Party shall encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks."[25]

21 These principles include limitation on collection, choice, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability.

22 The adoption of an adequacy decision involves a proposal from the European Commission, an opinion of the European Data Protection Board, approval from EU countries, and adoption of the decision by the European Commission. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en and https://trade.ec.europa.eu/access-to-markets/en/content/digital-trade-eu-trade-agreements-0).

23 https://trade.ec.europa.eu/access-to-markets/en/content/digital-trade-eu-trade-agreements-0; https://trade.ec.europa.eu/doclib/docs/2020/november/tradoc_159040.pdf

24 www.euractiv.com/section/data-protection/news/commission-not-naive-about-uks-data-ambitions-reynders-assures-meps.

25 Article 19, #7 (www.dfat.gov.au/trade/agreements/in-force/safta/Pages/singapore-australia-fta).

3. Enforce your own laws: Spam, privacy, and consumer protection

Most digital trade agreements have language that requires signatories to enforce their own laws on spam, privacy, and consumer protection. Such a strategy probably works well when signatories have long experience with internet or data governance. But many nations do not have either such laws or the funds, will or capacity to enforce them. Moreover, such an approach does little to foster international operability of regimes.

For example, many but not all countries have laws that ban spam.[26] In 2006, the members of the OECD issued recommendations on cooperation to address spam. They acknowledged that spam undermined the trust and consumer confidence "which is a prerequisite for the information society and for the success of e-commerce", and that it led to "economic and social costs". They also recognised that spam poses unique challenges for law enforcement in that senders can easily hide their identity, forge the electronic path of their email messages, and send their messages from anywhere in the world to anyone in the world, thus making spam a uniquely international problem that can only be efficiently addressed through international co-operation. The signatories agreed that they must cooperate to investigate and enforce cross-border spam problems (OECD 2006).

Most digital trade agreements also include language the requires firms to obtain the personal consent of consumers to receive spam, their right to opt out from receiving unwanted messages, and appropriate recourse if suppliers do not respect such regulations.[27] For example, the EU–UK Trade and Cooperation Agreement states that "[e]ach Party shall ensure that users are effectively protected against unsolicited direct marketing communications", but it does not delineate how. It also says spam is not illegal but that "each Party shall ensure that direct marketing communications are clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable users to request cessation free of charge and at any moment". Finally, users must have a form of redress (European Commission 2020). Australia–Singapore goes further, noting that "[e]ach Party shall provide recourse against a supplier of unsolicited commercial electronic message and the parties should cooperate in issues regarding spam".[28]

26 https://en.wikipedia.org/wiki/Email_spam_legislation_by_country

27 For example, US-Japan, Article 16 states that "[e]ach Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or (b)require the consent, as specified in its laws and regulations, of recipients to receive commercial electronic messages. 2.Each Party shall provide recourse against suppliers of unsolicited commercial electron" (https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf) CUSMA, Article 19.13 states "[e]ach Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic communications. 2. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic communications sent to an electronic mail address that messages that do not comply with the measures adopted or maintained pursuant to paragraph 1" (www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf).

28 Australia-Singapore, Article 19.

4. Bans on certain practices

Almost every digital trade agreement contains rules that forbid certain practices that might discriminate against foreign providers of data services (and in so doing impede market access). Hence, most such agreements ban performance requirements and data (or server) localisation policies. The EU–UK Agreement says cross-border data flows shall not be restricted by data localisation strategies and a Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party.[30] Recent US and Canadian trade agreements ban 'performance requirements' for source code. For example, US–Japan states that "[n]either Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory." It then allows an exception for a specific investigation, enforcement action, or judicial proceeding, subject to safeguards against unauthorised disclosure.[31] EU agreements have similar language.[32] But it is unclear why these practices are regulated by trade agreements, and not others, such as government use of malware or apps to spy on their citizens.

Table 1 compares recent trade agreements and how they address these issues.

THE GAPS IN THE CURRENT MODEL FOR ADDRESSING BARRIERS TO CROSS-BORDER DIGITAL TRADE

Digital trade agreements address some of the barriers encountered by market actors online. However, these agreements say nothing about other potential barriers to trade, including filtering and blocking, cybersecurity risks such as malware and DDOS attacks, regulations such as content moderation that are used to limit disinformation, and internet shutdowns.

If these potential barriers were to be governed by trade agreements, policymakers could potentially increase both trade and economic growth (OECD 2020: 11-12). Based on 2014 estimates, the US International Trade Commission found that decreasing barriers to cross-border data flows would increase US GDP by between 0.1% and 0.3% (USITC 2014). Table 2 illustrates some of these barriers.

30 Title III, Digital Trade p. 116, (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948119/EU-UK_Trade_and_Cooperation_Agreement_24.12.2020.pdf)

31 See US-Japan, Article 17, (https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf).

32 "No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party".

TABLE 1 THE LATEST DIGITAL TRADE AGREEMENTS AND WHAT THEY SAY ABOUT DIGITAL PROTECTIONISM

Provision	USMCA	EU-UK TCA	CPTPP	DEPA	AU/Sing DEA	US-Japan DTA	WTO draft text
Language explicitly encouraging cross-border data	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GAT/GATS exceptions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enforce domestic laws regarding privacy	Yes	Yes	Yes	Yes	Yes	Yes	No consensus yet[29]
Enforce domestic law regarding consumer protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enforce domestic laws regarding spam	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bans on performance requirements such as sharing source code and/or algorithms	Yes	Yes, source code only	Yes, source code only	Yes	Yes	Yes	Not clear yet
Ban on data localization	Yes	Yes	Yes	Yes	Yes	Yes	Not clear yet
Regulations banning divulgence of encryption	No	No	No	Yes	Yes	Yes	Yes

Source: Table by Andrew Kraskewicz with S. Aaronson.

29 See pages 27 and 28 of online draft text, which sources at WTO confirmed is legitimate but out of date as of February 2021.

TABLE 2 POTENTIAL BARRIERS TO CROSS-BORDER DATA FLOWS NOT YET ADDRESSED IN TRADE AGREEMENTS

Future barriers	Market trade effect	Disguised restriction on trade	In trade agreement
Data-sharing rules	Violate MFN, national treatment	Maybe	No
Algorithmic regulation (right to an explanation, avoid discriminatory outcomes, etc.)	Violate MFN, like-product national treatment	Maybe	No (protect public morals, social stability? w/ exception?)
Competition policies	Violate MFN	Maybe	No
Policies to limit disinformation	Violate MFN, like product	Maybe	No
Privacy label for apps (as in Apple app store)	Violate MFN, like product	Maybe	No
Censorship	Violate market access, may affect internet stability	Maybe	No (US is investigating)
Cybersecurity rules	Impede market access and discriminate among foreign and domestic providers	Maybe	Aspirational language encouraging cooperation

The potential barriers listed in the table will not be easy for nations to address in trade agreements.

1. **Data sharing**. Many nations do not yet have data-sharing rules (i.e. rules delineating how individuals, civil society groups, firms and governments can share and reuse various types of data including personal data). Without such rules, these nations are less likely to foster innovation and forgo economic growth.[33] But the rules could be designed in a discriminatory manner, favouring local companies over foreign ones.

2. **Algorithmic regulation**. Government officials may not yet be aware of the potential dangers of using algorithms to make decisions about access to credit or disinformation and will likely want to address this first at home before they do so internationally.

3. **Competition policy**. Although policymakers have at times tried to include competition policies in international trade agreements – an example being cartel policies in the International Trade Organization (ITO) – in general, competition policymaking is national, reflecting national norms of fair or unfair competition. Thus, trade policymakers may not view the lack of competition policy coherence and coordination as a trade issue.

4. **Strategies to address disinformation**. Policymakers may disagree on how to define problems such as disinformation. But national strategies to address disinformation that flows across borders could distort trade. Divergent approaches could create barriers to digital trade. Nations would benefit if they tried to coordinate such strategies through a shared approach to regulation.

5. **Privacy labels**. Increasingly, firms such as Apple want to be responsible stewards of personal data and are using their data protection strategies as a means of signalling and competitive advantage. These labels are supposed to provide users with background information about what types of personal data apps and websites utilise, so users can make sound decisions about whether or not to download an app or go to a site. But firms may not be honest about the information and consumers may find such information confusing, incomplete and inaccurate. The labels may violate various consumer protection and commercial speech regulations. Domestic providers may find it easier to influence the labels.[34] Consequently, privacy labelling could be a trade barrier.

6. **Censorship.** When nations censor the internet, they not only impede access to information, but they may also impede market access.

33 www.weforum.org/agenda/2019/08/private-data-public-is-a-good-thing/; https://digital-strategy.ec.europa.eu/en/policies/strategy-datal

34 https://news.bloomberglaw.com/tech-and-telecom-law/apples-app-privacy-disclosure-regime-risks-ftc-legal-scrutiny

7. **Cybersecurity rules**. Nations must collaborate to protect data and keep the internet stable. Ideally, they should work towards trusted interoperable rules, because divergent approaches risk creating barriers to digital trade. These barriers may include unique standards, requirements for localisation of data or technology supply, and overreaching national security protections. Such policies may discriminate among nations and/or firms and undermine market access (Meltzer and Kerry 2019; Peng 2015).[35] In the draft WTO text, members address cybersecurity by calling for risk-based over regulatory-based approaches and encouraging cybersecurity cooperation.[36]

To illustrate the difficulty of developing shared positions on whether or not these potential barriers should be addressed by trade agreements, I focus on three of these issues in greater detail. I chose these three because they also have significant human rights and democracy effects, and hence should garner greater attention. Moreover, the three are likely to yield different trade policy rule-making outcomes. The US is already examining whether censorship is a trade barrier. Internet shutdowns have much wider internet effects then censorship, but because of that wider effect, policymakers could engage in a broader discussion about how and when nations can use shutdowns. Finally, nations will likely struggle to define disinformation, yet there are some policy solutions that could easily be added to the language on spam in most trade agreements.

Censorship

All nations censor speech when it may be dangerous or when it violates national norms and laws. However, when governments suppress or prohibit speech or other communication, they may be undermining the internationally accepted human right of freedom of expression. Governments can use technical or legal means to censor. As example, democratic nations including the US,[37] India[38] and Brazil[39] have also restricted access to apps and various platforms through such strategies. Meanwhile in 2020, authorities in Chad, Kazakhstan, Sri Lanka, and Venezuela choose to block specific social media or messaging applications or prevent traffic to livestreaming platforms (Human Rights Watch 2021).

Some argue that government-mandated content moderation is a form of censorship. Content moderation empowers private actors to establish community guidelines for their sites and demand that users seeking to express their viewpoints are consistent with that particular community's expectations of discourse (Walter 2016). For example, Germans are deeply concerned about hate speech online. Germany's Network Enforcement Act

35 www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm
36 www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf (pp. 56, 58).
37 The Trump Administration tried to ban two Chinese owned apps for alleged national security reasons, but the courts did not uphold the bans and the Biden Administration has abandoned this plan (www.bbc.com/news/technology-54205231 and www.bankinfosecurity.com/biden-assesses-us-policies-on-china-cybersecurity-issues-a-16000).
38 www.reuters.com/article/us-india-china-apps/india-retains-ban-on-59-chinese-apps-including-tiktok-idUSKBN29U2GJ
39 https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/

(NetzDG) requires platforms with over two million registered users to take down illegal content, including hate speech and "defamation of religions", if individuals flag it. Any content which is "manifestly unlawful" must be removed within 24 hours. A 2019 study found that after the law came into effect, at least 13 countries, in addition to the EU, adopted or proposed models of intermediary liability and content moderation broadly similar to the NetzDG approach (Mchangama and Fiss 2019, Roth 2020). But is the law protectionist? Protectionism was unlikely the intent of the law, although it may be the outcome. The German law applies only to the biggest platforms with the most users, which are generally based in the US and China, raising their compliance costs.

In 2020, the US Senate held a hearing on whether the Great Firewall of China constituted a form of censorship (through technical and legal means). According to Nigel Corey, "U.S. firms face a complicated, opaque, and changing regulatory framework tied to content moderation and information control that together makes for a very difficult and different business environment. Moreover, in many cases, China's approach to censorship is unwritten, with enforcement often being arbitrary and delegated to private firms. This is in large part a conscious decision to avoid WTO sanctions which would be much easier to put in place if the rules are on paper" (Corey 2020: 6-7).

No trade agreement thus far says anything explicit about censorship through legal or technical means. The legal scholar Anupam Chander has noted that censorship is not necessarily a market access or a national treatment violation. But when governments restrict access to foreign sites, require foreign information service providers to route their offerings through special traffic cops, or require local internet service providers to deny access to certain foreign services, these governments may be acting in a discriminatory manner in blocking market access (Chander 2009). Policymakers have never challenged censorship in a trade dispute. However, the US (and, for a time, the EU) has at times flirted with the idea of examining censorship as a trade barrier after human rights groups (and firms) complained about the direct and indirect effects of China's Great Firewall (Google 2010, Aaronson 2015, Economy 2018).

After the 2020 hearing, Charles Grassley, then the Chairman of the Senate Finance Committee, requested that the US International Trade Commission examine if censorship is a barrier to trade. The US thus became the first nation to seek both qualitative and quantitative evidence of such costs. The requestors defined censorship broadly as "the prohibition or suppression of speech or other forms of communication", and stated that foreign governments use many tools to carry out censorship, including technological measures that restrict digital trade. The study is designed to identify and describe various foreign censorship practices, in particular those that impede trade or investment in key foreign markets. Paraphrasing, the description of these practices should include the

evolution of censorship policies and practices over the past five years in key foreign markets' any elements that entail extraterritorial censorship, and the roles of governmental and non-governmental actors in implementation and enforcement of censorship. [40]

Internet throttling and shutdowns

To maintain control over the internet, some nations such as Indonesia and Iran frequently slow or throttle the internet within their borders. By slowing internet speeds to a crawl, policymakers can more easily manipulate and monitor online activities (Human Rights Watch 2021). But they may also distort trade by discriminating among foreign and domestic service providers and/or by limiting market access.

For example, under Russia's sovereign internet law, it is illegal to send certain types of data to servers abroad. In March 2021, Russia ordered Twitter to be slowed down because it failed to remove banned content (Dixon 2021). According to the human rights NGO Access Now, after Russia throttled Twitter, Russian users began reporting the slowing down of multiple websites and online services. Experts later confirmed that over 40,000 domains containing "t.co" (Twitter's shortened domain name) had been affected. When Russia throttled Twitter, it also slowed down the websites of key governmental institutions, including the Kremlin and the Russian State Duma, as well as major platforms and services including Yandex, Google, YouTube, and Qiwi.[41] The Russian internet regulator, Roskomnadzor, blamed some of the site blockings on a fire at a cloud services firm OVHcloud in Strasbourg, France. As Google was also affected, it investigated and asserted that "[w]e have no evidence to indicate that the fire in OVHCloud's data centre, or Google's own infrastructure, was the root cause of this incident. We believe the cause of this incident was a misconfiguration of the routers at a local third-party internet service provider."[42] However, as of this writing, Netblocks, an NGO that examines such activities, has not yet concluded that the government throttling of Twitter and the reported internet malfunctions are related.[43]

Internet shutdowns are much more drastic in their effects on both human rights and market access than censorship. Access Now defines internet shutdowns as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable for a specific population or within a location, often to exert control over the flow of information. [44] Internet shutdowns have both direct and indirect effects. They can hamper productivity, frustrate business confidence and trust, and raise firm and consumer costs (Deloitte 2016). Internet shutdowns can lead to lost business and tax

40 US ITC, USTIC to Investigate Effect of Foreign Censorship on U.S. Businesses", US ITC, January 2021 (www.usitc.gov/press_room/news_release/2021/er0126ll1708.htm); and a letter by Charles Grassley (https://usitc.gov/research_and_analysis/off_req_ltr_censorship.pdf)

41 https://netblocks.org/reports/internet-disrupted-in-russia-as-regulator-imposes-new-measures-l8WxaQAO

42 www.businessinsider.com/google-russia-internet-outage-fire-data-center-twitter-censorship-censor-2021-3

43 https://netblocks.org/reports/internet-disrupted-in-russia-as-regulator-imposes-new-measures-l8WxaQAO

44 Access Now found that in 2019, 1,706 days of internet access were disrupted by 213 internet shutdowns across 33 countries (www.accessnow.org/cms/assets/uploads/2021/02/Read-Me_-How-to-view-the-Access-Now-Internet-Shutdown-Tracker-Updated-Mar-2021.pdf).

revenues and lower worker productivity (West 2016). When officials place limitations on which firms can participate in the network, they reduce its overall size and generativity. Shutdowns can also increase costs to local businesses, affect global value chains and reduce technology diffusion, thereby undermining development and trade (Box 2016: 2).

Internet shutdowns represent a growing cost to the digital economy. In 2016, Darrell West of Brookings estimated that shutdowns cost the global economy $2.4 billion (West 2016). In 2019, researchers found some 21 countries shut down the internet within their boundaries, and that these shutdowns cost some $8.05 billion.[45] A 2020 study found that 21 countries shut down the internet in 2020, costing some $4 billion.[46]

As a result of these shutdowns, some 268 million people in 2020 were unable to access the internet at various times. Some 42% of shutdowns in 2020 were associated with additional human rights abuses – 29% were associated with restrictions on freedom of assembly, 15% with election interference, and 12% with infringements on freedom of the press.[47]

Policymakers may only intend to control the internet within their borders, but such actions often resonate beyond their borders. Shutdowns undermine access to information, reducing innovation and the ability of citizens to monitor and hold their governments to account (OECD 2016, Aaronson 2018a). They may also reduce internet stability and diminish the predictability of data flows (Google 2010, OECD 2016). In so doing, shutdowns essentially export these effects to other markets (Aaronson 2018a).

Internet shutdowns effectively censor both individuals and firms. Yet internet shutdowns are different from censorship because shutdowns do not discriminate regarding content; instead, they block all content. They also encompass all forms of digital communication, from email to social networks. Internet shutdowns also typically directly affect mobile phone services. Finally, internet shutdowns are not aimed at one piece of content but rather at the act of communication (Wagner 2018: 3920-3921).

We know of no attempt to define internet shutdowns as a trade barrier. As with censorship, governments could justify their actions under the exceptions. But given the broader effects of internet shutdowns, it would be interesting to see if a dispute settlement body would find such actions to be discriminatory.

Disinformation as a trade barrier

Disinformation can be defined as information designed to mislead, deceive, or polarise (Park Advisors 2019). Disinformation is not new, but the business model underpinning many social networking platforms has facilitated its spread. Netizens around the world have turned to Facebook, Google, WeChat and other sites, apps, and browsers for

45 www.top10vpn.com/cost-of-internet-shutdowns-2019/
46 Samuel Woodhams and Simon Migliano used Netblocks tools to estimate these costs. (www.top10vpn.com/cost-of-internet-shutdowns/).
47 www.top10vpn.com/cost-of-internet-shutdowns/

information and increasingly for their news.[48] Many of these sites, apps, and browsers provide their services to netizens for free; instead they depend on ads for revenues and profits.[49] Critics accuse many social networking platforms of feeding their users divisive content to gain their attention and to increase the time they spend on the platform, which in turn encourages more advertisers (Ghosh et al. 2021). Meanwhile, the ads provide the firms with a global revenue stream that both incentivises and sustains the spread of disinformation.[50]

Disinformation is dangerous to both human rights and democracy. It interferes with the public's ability to seek, receive and impart information and ideas regardless of frontiers (Cedar Partners 2020, Infield 2020). Disinformation is also dangerous for economic stability. As it spreads, it can affect the reputations of firms and stock prices (Carvalho et al. 2009, Insikt Group 2019) and alter economic decisions,[51] undermine public health and belief in science, and reduce trust in institutions (University of Baltimore and Cheq 2019, Infield 2020). In a December 2020 study, the Oxford Internet Institute analysed survey data from 154,195 participants living in 142 countries and found that more than half (53%) of regular internet users are concerned about disinformation (Knutila et al. 2020).

Disinformation is increasingly a trade problem, as individuals in one country disseminate disinformation about and in other countries (Park Advisors 2019, OHCHR 2020). Moreover, it provides an example of how national regulations might yield digital trade distortions. Many nations have adopted a wide range of strategies to mitigate disinformation, including platform regulation, personal data protection rules, competition policies, investment rules, technological fixes, and citizen education strategies. With so many different approaches, policymakers will eventually obtain a clearer understanding of what works and what does not. However, this patchwork may not be effective in mitigating cross-border disinformation. Moreover, the lack of a coherent approach could lead to trade distortions as well as spillover effects on internet openness and generativity (OECD 2016, World Economic Forum 2020). Such strategies may be seen as trade-distorting because many of the regulations are designed to govern applications with large user bases. These platforms tend to be US or China based. Hence, they appear discriminatory. Moreover, there is growing evidence that the data giants have acted at the national level to weaken and contest domestic regulations aimed at addressing disinformation. Firms may be trying to game the system.

48 For example, in 2018 some 40% of Facebook users get their news from the platform (www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/ and www.accc.gov.au/media-release/lack-of-competition-in-ad-tech-affecting-publishers-advertisers-and-consumers).

49 Digital advertising is, in essence, how consumers' attention and data are monetised.

50 Global Disinformation Index (https://disinformationindex.org/wp-content/uploads/2020/10/Oct-2nd-DisinfoAds-Brands-next-to-Anti-SemitismGlobalist-Conspiracy-theories.pdf).

51 www.nytimes.com/2021/01/29/technology/commercial-disinformation-huawei-belgium.html

If policymakers were to develop a coordinated and effective international approach, they might possibly reduce these costs and bolster trust online. A recent study found that unilateral data regulations can either raise or reduce global welfare, but a coordinated approach would yield substantial gains (Chen et al. 2020: 4).

Existing digital trade agreements may provide a path forward by building on their language regulating spam discussed earlier.[52] Spam and disinformation are quite different, but both are forms of unsolicited electronic transmissions and both are often disseminated across borders by bots (Aaronson 2021). Policymakers could add to this language by banning spambots and by encouraging regulatory cooperation and coherence in their digital trade agreements.

FOOD FOR THOUGHT: WE NEED A RETHINK ABOUT LEGITIMATE REGULATION AND DIGITAL PROTECTIONISM

The OECD reviews barriers to digital trade annually. In 2019, it noted that its indices revealed a "tightening regulatory environment highlighting that further international cooperation and dialogue is needed to maximise the benefits of digitalization" (Ferencz 2019). The WTO concurred – in its *2020 World Trade Report*, the WTO Secretariat noted a catch-22 in the global economy: "the increasing importance of data as an input in production and the fluidity of data is leading to increasing demands for new international rules on data transfers, data localization and privacy… At the same time, the winner-takes-all characteristics of certain digital industries could lead to policy responses that raise tensions between countries and introduce unnecessarily high market barriers" (WTO 2020: 11-12).

These international organisations are clearly warning that the world would benefit from a broader discussion of the relationship between domestic regulation and digital trade rules. Yet, recent trade agreements only cover some potential barriers to data flows, including personal data protection, consumer regulation, spam, data localisation and source code performance requirements. The most recent trade agreements do not address other barriers such as censorship, shutdowns, disinformation or filtering.

Not only have policymakers failed to defined or addressed digital protectionism, but they have also failed to develop a strategy to address it. There is no international shared law governing many of these alleged barriers, so telling nations to enforce their own laws is likely to result in a growing number of trade disputes. Moreover, many nations do not have the expertise, will or funds to draft and enforce laws on privacy disinformation or cybersecurity. They will need help to do this (Aaronson 2019). Finally, requiring nations to enforce their own laws without an internationally accepted set of principles or a draft law is unlikely to yield the interoperability needed to maintain a trusted and stable internet.

52 https://en.wikipedia.org/wiki/Email_spam_legislation_by_country

Hence, policymakers need to figure out ways to encourage nations to adopt shared norms for internet stability, even if they do not achieve common language through the WTO or other trade agreements.

Moreover, policymakers have not addressed what to do about these alleged barriers. As noted earlier, when the Global Digital Protectionism project examined six case-study countries, no government had come up with a policy to address the following questions:

- If a policy is trade distorting, who is injured?
- How can the government compensate those who are injured without further distorting trade?
- How should the government respond to these barriers that remain unaddressed in trade agreements? Should nations use tariffs to respond to trade distorting app bans or internet shutdowns?[53]

The Digital Trade and Data Governance Hub will update these findings later in 2021, with the data governance mapping project.[54] However, as of this writing, we are unaware of any government that has answered these questions and clarified their strategy in public.

Policymakers need to address these barriers if they want to maintain trust online. A 2018 poll in 18 countries from BBC News found that 79% of respondents said they worried about what was fake and what was real on the internet.[55] The Canadian think tank CIGI surveyed some 20,000 netizens around the world in 2019 and that found social media companies are the leading source of user distrust in the internet — surpassed only by cybercriminals — with 75% of those surveyed citing Facebook, Twitter, and other social media platforms as contributing to their lack of trust.[56]

Trade negotiating is never easy, and it is especially difficult to negotiate data because of its unique properties. Below are some suggestions that might build such trust while addressing digital protectionism.

Trade policymakers should:

- challenge trade distorting policies in dispute settlement to better understand the rules and their limits;
- tighten how and when nations can use the exceptions;

53 www.digitaltradepolicy.org/
54 https://datagovhub.elliott.gwu.edu/the-global-data-governance-mapping-project/
55 www.bbc.com/news/technology-41319683
56 The 2019 CIGI-Ipsos Global Survey on Internet Security and Trust was conducted between 21 December 2018 and 10 February 2019, and involved 25,229 internet users in Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Russia, South Africa, Republic of Korea, Sweden, Tunisia, Turkey and the United States (https://www.cigionline.org/internet-survey-2019).

- encourage greater regulatory coherence and cooperation, particularly on disinformation and competition policies;
- elevate the importance of data governance and fund and build data regulatory capacity in the developing world; and
- require nations to report on the barriers to cross-border data flows they encounter as well as those they may have erected at their WTO trade policy reviews.

REFERENCES

Aaronson, S (2015), "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-border Data Flows, Human Rights and National Security", *World Trade Review* 14(4): 671–700.

Aaronson, S (2018a), "What are we Talking About When we Talk about Digital Protectionism?", *World Trade Review* 18(4): 541-577.

Aaronson, S (2018b), "Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows", CIGI Paper No. 197 (www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows).

Aaronson, S (2019), "Data Is a Development Issue", CIGI Paper No. 223 (www.cigionline.org/publications/data-development-issue).

Aaronson, S (2020), "Data is Dangerous", CIGI Paper No 241 (www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves).

Aaronson, S (2021), "Could Trade Agreements Help Address the Wicked Problem of Cross-Border Disinformation?", GICI, forthcoming.

Aaronson, S and P LeBlond (2018), "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO", *Journal of International Economic Law* 21(2): 245-272 (https://doi.org/10.1093/jiel/jgy019).

Aaronson, S and T Struett (2020), "Data is Divisive: A History of Public Communications on E-Commerce, 1998-2020", CIGI Paper No. 247 (www.cigionline.org/publications/data-divisive-history-public-communications-e-commerce-1998-2020).

Belton, K (2019), *Smart Factories: Issues of Information Governance*, Manufacturing Policy, Initiative School of Public and Environmental Affairs, Indiana University (https://manufacturingpolicy.indiana.edu/doc/Smart%20Factories.pdf).

Box, S (2016), "Internet Openness and Fragmentation: Towards Measuring the Economic Effects", CIGI Paper No. 36, CIGI and Chatham House (www.cigionline.org/sites/default/files/gcig_no.36_web.pdf).

Buchser, M and J Hakmeh (2019), "Tackle the 'Splinternet'", Chatham House, 12 June 12 (www.chathamhouse.org/2019/06/tackle-splinternet).

Burri, M (2013), "Should There Be New Multilateral Rules for Digital Trade?", Think piece for the E15 Expert Group on Trade and Innovation, International Centre for Trade and Sustainable Development (https://ssrn.com/abstract=2344629).

Carvalho, C, N Klagge, and E Moench (2009), "The Persistent Effects of a False News Shock", Federal Reserve Bank of New York Staff Reports No. 374 (revised March 2010).

Casalini, F and J López González (2019), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers No. 220 (https://doi.org/10.1787/b2023a47-en).

Cedar Partners (2020), Platform Accountability: Global Challenges and Opportunities (https://drive.google.com/file/d/1S4MBS8VmKCiqqBXLdANiF4ijaqfvq-mY/view).

Chander, A (2009), "International Trade and Internet Freedom", *America Society of International Law* 102: 37 (https://ssrn.com/abstract=1536873).

Chander, A and U P Le (2014), "Breaking the Web: Data Localization vs. the Global Internet", UC Davis Legal Studies Research Paper No. 378 (https://ssrn.com/abstract=2407858).

Chander, A and U P Le (2015), "Data Nationalism", *Emory Law Journal* 64(3) (https://ssrn.com/abstract=2577947).

Chazan, G (2019), "Angela Merkel urges EU to seize control of data from US tech titans", *Financial Times*, 12 February (www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca).

Chen, Y, X Hua and K E Maskus (2020), "International Protection of Consumer Data", CESifo Working Paper No. 8391 (https://ssrn.com/abstract=3642389).

Ciuriak, D (2019), "World Trade Organization 2.0: Reforming Multilateral Trade Rules for the Digital Age", CIGI Policy Brief No. 152 (www.cigionline.org/sites/default/files/documents/PB%20no.152_3.pdf).

Corey, N (2018), "The Global Rise of 'Data Localism'", *Brink Magazine*, 31 January (www.brinknews.com/the-global-rise-of-data-localism/).

Corey, N (2019), "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It is Used", Not Where It's Stored, 1 April (https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where).

Corey, N (2020), Testimony Before the Senate Subcommittee on International Trade, Customs, and Global Competitiveness of the Committee on Finance Hearing on "Censorship as a Non-Tariff Barrier to Trade", 30 June (www2.itif.org/2020-censorship-ntb.pdf).

Daigle, L (2015), "On the Nature of the Internet", Centre for International Governance Innovation.

Deloitte (2016), *The economic impact of disruptions to Internet connectivity: A report for Facebook* (www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html).

de la Chapelle, B and P Fehlinger (2016), "Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation", Centre for International Governance Innovation, 1 April.

Dixon, R (2021), "Why Russia is tightening its grip on social media", *The Washington Post*, 12 March (www.washingtonpost.com/world/2021/03/12/russia-social-media-putin-opposition/).

Drake, W, V Cerf, and W Kleinwächter (2016), *Internet Fragmentation: An Overview*, World Economic Forum (www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf).

Economy, E C (2018), "The great firewall of China: Xi Jinping's internet shutdown", *The Guardian*, 29 June (www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown).

European Commission (2020), "Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part", COM(2020) 857 final, 25 December (https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-857-F1-EN-ANNEX-1-PART-1.PDF).

Fefer, R (2019), "Digital Trade and U.S. Trade Policy", CRS R44565, Congressional Research Service, 21 May (https://fas.org/sgp/crs/misc/R44565.pdf).

Ferencz, J (2019), "The OECD Digital Services Trade Restrictiveness Index", OECD Trade Policy Papers, No. 221 (https://doi.org/10.1787/16ed2d78-en).

Ghosh, D, L Gorman, B Schafer, and C Tsao (2021), *The Weaponized Web: Tech Policy Through the Lens of National Security*, Alliance for Securing Democracy and the Kennedy School (https://securingdemocracy.gmfus.org/wp-content/uploads/2020/12/The-Weaponized-Web.pdf).

Goldman, E (2011), "The OPEN Act: Significantly Flawed, but More Salvageable than SOPA/PROTECT IP", *Ars Technica*, 12 December (https://arstechnica.com/tech-policy/2011/12/the-open-act-significantly-flawed-but-more-salvageable-than-sopaprotect-ip/).

Google (2010), "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information" (www.benton.org/headlines/enabling-trade-era-information-technologies-breaking-down-barriers-free-flow-information).

Human Rights Watch (2021), "Shutting Down the Internet to Shut Up Critics", *World Report 2020* (www.hrw.org/world-report/2020/country-chapters/global-5).

Infield, T (2020), "Americans Who Get News Mainly on Social Media Are Less Knowledgeable and Less Engaged", *Trust Magazine*, 16 November, Pew (www.pewtrusts.org/en/trust/archive/fall-2020/americans-who-get-news-mainly-on-social-media-are-less-knowledgeable-and-less-engaged).

Insikt Group (2019), *The Price of Influence: Disinformation in the Private Sector*, 30 September (https://go.recordedfuture.com/hubfs/reports/cta-2019-0930.pdf).

Knutila, A, L -M Neudert and P N Howard (2020), "Global Fears of Disinformation Perceived Internet and Social Media Harms in142 Countries", COMPROP Data Memo 2020.8, Computational Propaganda Project (https://mediawell.ssrc.org/2020/12/15/global-fears-of-disinformation-perceived-internet-and-social-media-harms-in-142-countries-oxford-internet-institute/).

López González, J and J Ferencz (2018), "Digital Trade and Market Openness", OECD Trade Policy Papers, No. 217 (https://doi.org/10.1787/1bd89c9a-en).

Macedoni, L and A Weinberger (2019), "Quality Heterogeneity and Misallocation: The Welfare Benefits of Raising your Standards" (https://ssrn.com/abstract=3436156 or http://dx.doi.org/10.2139/ssrn.3436156).

Maskus, K E and J H Reichman (2004), "The Globalization of Private Knowledge Goods and the Privatization of Global Public Goods", *Journal of International Economic Law* 7: 279-320 (https://ssrn.com/abstract=692902).

Mchangama, J and J Fiss (2019,) *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship*, Justitcia (http://justitia-int.org/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf).

Meltzer, J and C Kerry (2019), "Cybersecurity and digital trade: Getting it right," Brookings, 18 September (www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/).

Monteiro, J-A and R Teh (2017), "Provisions on Electronic Commerce in Regional Trade Agreements", WTO Working Paper ERSD-2017-11.

OECD (2006), "OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam", 13 April (www.oecd.org/sti/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm).

OECD (2016), "Economic and Social Benefits of Internet Openness", OECD Digital Economy Papers 257 (www.oecd-ilibrary.org/science-and-technology/economic-and-social-benefits-of-internet-openness_5jlwqf2r97g5-en).

OECD (2020), *Mapping Approaches to Data and Data Flows*, Report for the G20 Digital Economy Task Force, Saudi Arabia 2020.

OHCHR – Office of the High Commissioner for Human Rights (2017), "Joint Declaration on Freedom of Expression and Fake news, Disinformation and Propaganda", 3 March (www.ohchr.org/Documents/Issues/Expression/JointDeclaration3March2017.doc).

OHCHR (2020), *Report on Disinformation* (www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Report-on-disinformation.aspx).

Park Advisors (2019), "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age", March (www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf).

Peng, S-Y (2015), "Cybersecurity Threats and the WTO National Security Exceptions", *Journal of International Economic Law* 18(2): 449-478 (https://ssrn.com/abstract=2640447).

Roth, K (2020), *Shutting Down the Internet to Shut Up Critics*, Human Rights Watch World Report (www.hrw.org/world-report/2020/country-chapters/global-5).

UNCTAD (2017) *Digitalization, Trade and Development*, Information Economy Report, 2017 (https://unctad.org/en/PublicationsLibrary/ier2017_overview_en.pdf).

UNCTAD (2020), "Digital platforms and value creation in developing countries: Implications for national and international policies", Note by the UNCTAD Secretariat, 19 February (https://unctad.org/meetings/en/SessionalDocuments/tdb_ede4d2_en.pdf).

USITC – United States International Trade Commission (2014), *Digital Trade in the U.S. and Global Economies, Part 2*.

University of Baltimore and Cheq (2019), *The Economic Cost of Bad Actors on the Internet: Fake News in 2019* (www.cheq.ai/fakenews).

Wagner, B (2018), "Understanding Internet Shutdowns: A Case Study from Pakistan", *International Journal of Communication* 12: 3917–3938.

Walter, J (2016), "Content Moderation Is Not Synonymous With Censorship", *Public Knowledge*, November (www.publicknowledge.org/blog/content-moderation-is-not-synonymous-with-censorship).

Weber, S (2017), "Data, Development and Growth", *Business and Politics* 19(3): 397-423 (www.cambridge.org/core/journals/business-and-politics/article/data-development-and-growth/DC04765FB73157C8AB76AB1742ECD38A).

West, D (2016), "Internet shutdowns cost countries $2.4 billion last year", Brookings, 6 October (www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/).

World Bank (2016), *World Development Report 2016: Digital Dividends* (www.worldbank.org/en/publication/wdr2016).

World Economic Forum (2019), *Exploring International Data Flow Governance*, December (www.weforum.org/whitepapers/exploring-international-data-flow-governance).

World Economic Forum (2020), *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows* (www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf).

WTO – World Trade Organization (2020), *World Trade Report 2020: Government policies to promote innovation in the digital age* (www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20_e.pdf).

ABOUT THE AUTHOR

Susan Ariel Aaronson is Research Professor and Director of the Digital Trade and Data Governance Hub at the George Washington University and a Senior Fellow at the Canadian think tank Centre for International Governance Innovation (CIGI).

CHAPTER 6

Governing cross-border data flows beyond trade agreements to support digital trade: Inspiration from international financial standards-setting bodies

Patrick Leblond
University of Ottawa

INTRODUCTION

Nowadays, trade agreements cannot avoid including chapters covering digital trade.[1] The latest major agreement to do so is the Regional Comprehensive Economic Partnership (RCEP), which was signed by its Asia-Pacific members in November 2020. For their part, a significant number of WTO members are actively negotiating a plurilateral agreement on 'trade-related aspects of electronic commerce'.[2]

The reason for these provisions in trade agreements is that digital trade has been growing rapidly (McKinsey 2016, WTO 2018, OECD 2019). These provisions focus most of their attention on the potential obstacles that national regulations of the digital sphere pose to such trade. Regulations restricting the flow of data (personal, business and government) across borders are considered an important impediment to trade (Rentzhog and Jonströmer 2014, Cory 2017, Ciuriak and Ptashkina 2018, Aaronson 2019a). For instance, Rentzhog (2015), in a study of Swedish companies from a wide range of sectors, found that moving data across borders easily was crucial for the well-functioning of these firms' global value chains. Restrictions on cross-border data flows are particularly problematic for digital trade (Ferracane and van der Marel 2019).

Trade agreements such as the RCEP, the Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP) and the United States–Mexico–Canada Agreement (USMCA), which replaced the North American Free Trade Agreement (NAFTA), recognise that policymakers face a tension between, on the one hand, generating the economic benefits associated with unfettered data flows across borders and, on the other

1 Aaronson and Leblond (2018) define digital trade as encompassing "digitally enabled transactions in trade in goods and services that can be either digitally or physically delivered involving consumers, firms, and governments" (p. 248).
2 https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.

hand, providing a trusting environment for individuals, firms and governments taking part in the data-driven economy. However, like in the other areas that they cover, these trade agreements aim to ensure that national regulations affecting data flows are not disguised protectionist measures that discriminate against foreign providers of digital goods and services in favour of domestic ones.[3] As such, the core principles of national treatment, most-favoured nation and transparency apply here as well. Although such trade agreements have the potential to limit the ability of governments to regulate data and the digital economy domestically (Leblond 2021), in this chapter I argue that they are unlikely to prevent national regulation from restricting cross-border data flows and, thus, digital trade between their member states.

The situation regarding trade in digital goods and services is akin to that of trade in financial services. Trade agreements covering financial services aim to ensure that the latter's liberalisation does not take place at the expense of the integrity and stability of each party's financial system or the protection of consumers and investors. This is why they contain a so-called 'prudential carve-out' (PCO), which allows parties to adopt or maintain regulatory measures for prudential reasons: first, to protect investors, depositors and policy holders, as well as financial service suppliers; second, to maintain the safety, soundness, integrity or financial responsibility of a financial institution or cross-border financial service supplier; and third, to ensure the integrity and stability of the parties' financial systems. In the GATS, the PCO is found in paragraph 2(a) of the Annex on Financial Services. There is significant ambiguity with respect to the PCO's scope of application in the GATS (Yokoi-Arai 2008, Mitchell et al. 2016, Cantore 2018, Papaconstantinou 2020). For instance, the notion of 'prudential' has been left undefined. As such, according to Yokoi-Arai (2008: 639), it leaves "the impression that financial liberalization may be subject to the discretion of members". The uncertainty of the PCO's scope of application in the GATS has led some countries to negotiate more specific language in their bilateral trade agreements (Cantore 2018: Chapter 4). For instance, NAFTA was the first such agreement to include a 'reasonableness test' for prudential measures (Cantore 2018: 116). Other agreements, such as the Comprehensive Economic and Trade Agreement between Canada and the EU, go further and explicitly refer to internationally agreed financial standards as benchmarks for determining if a prudential measure is justified or reasonable in case it discriminates against foreign financial service providers or investors (Mitchell et al. 2016: 811, Milano and Zugliani 2019: 175).

So, trade in digital goods and services shares the same kind of uncertainty around the scope of application of regulatory exceptions (or carve-outs) in trade agreements as does trade in financial services. However, contrary to financial markets, digital trade also suffers from the absence of internationally agreed standards to govern data-driven markets (Meltzer 2019). This means that there is no basis for assessing the legitimacy of national regulatory measures that would restrict trade in digital goods and services (e.g.

3 For an excellent discussion of digital protectionism, see Aaronson (2019a).

limits on cross-border data flows). Such a situation is highly problematic since, as I argue here, existing trade agreements ultimately leave it in the hands of a few panel members within a dispute settlement mechanism to resolve the uncertainty surrounding the scope of application of national data regulation versus unfettered cross-border digital trade.

Consequently, we risk ending up with one of two unsatisfactory scenarios. In the first scenario, member states are allowed to adopt whatever regulations they deem necessary to protect individuals, consumers, businesses and governments at the national level but at the expense of cross-border digital trade (Meltzer 2019). In the second scenario, digital trade is free to take place across borders – as a result of limiting national data regulations' scope of applicability – but at the expense of trust in data-driven markets. These two scenarios are derived from Leblond and Aaronson's (2019) data trilemma, which states that the following three elements cannot hold simultaneously: data flows freely across borders; national data protection laws and regulations that are distinct from those of other countries are in place; there is a high level of trust in the data environments among individuals, consumers, businesses and governments. Only two of the three elements can occur at the same time.[4] Strong national data protection laws and regulations should lead to high trust levels but, to do so, they risk imposing restrictions on cross-border data flows. Alternatively, if policymakers want to ensure the free flow of data across borders while maintaining national data policies, then they may have to accept weaker data protection measures, which could negatively affect trust. Finally, if policymakers want data to flow freely across borders while ensuring a high degree of trust surrounding the collection and use of data, then they either adopt another jurisdiction's regulatory standards (in order for data to flow freely with this jurisdiction and others with the same recognised standards) or they cooperate with governments in other countries to develop and enforce common, high-quality protection standards and regulations for personal as well as non-personal data (see also Meltzer 2019).

Therefore, in order to avoid the two above-mentioned scenarios that digital trade provisions in existing trade agreements – such as the CPTPP, the USMCA, the RCEP as well as the possible plurilateral agreement on trade-related aspects of electronic commerce at the WTO – are likely to produce, we need a separate international governance regime for cross-border data. Leblond and Aaronson (2019) argue that the best approach to obtaining 'free' cross-border data flows and high trust levels amongst consumers, businesses and governments in data-driven markets is to create a single data area with its own standard-setting and monitoring body, which, the authors suggest, could be called the 'International Data Standards Board'.[5] In other words, following the same logic that

4 The data trilemma draws inspiration from the financial trilemma (Schoenmaker 2013), which states that financial stability, financial integration and national financial policies cannot all occur simultaneously; only two of the three objectives can be combined at any given time.

5 Knake (2020) also argues for a 'digital trade zone' with common standards and practices in order to achieve online freedom, privacy and cybersecurity.

applies to financial regulation and trade in financial services, standards and regulations governing data within the single data area would be separate from the rules governing international trade in digital goods and services.

This chapter puts flesh on the bones of an International Data Standards Board and its functioning. To do so, it uses as a model the international architecture for governing finance. Before that, however, it makes the case that existing trade agreements and the WTO's possible agreement on trade-related aspects of electronic commerce are unlikely to be effective instruments for promoting international trade in digital goods and services. Either they will not stop governments from adopting national regulations, especially pertaining to data, that impede cross-border digital trade, or they will manage to undermine national regulations in favour of allowing digital trade to take place across borders without restrictions but at the expense of trust in data-driven markets, which will then lead market actors to seek to limit their involvement in digital trade beyond their national borders.

TRADE AGREEMENTS AND THE WTO ARE INEFFECTIVE TO GOVERN CROSS-BORDER DATA FLOWS

This section analyses the provisions regarding cross-border data flows found in the CPTPP, the USMCA and the RCEP, as well as the WTO's negotiations of an agreement on trade-related aspects of electronic commerce. The focus is on data-related provisions because cross-border data flows are deemed crucial for enabling digital trade, as discussed briefly in the introduction above. It is also important to note that the digital trade chapters in the USMCA and the RCEP are closely built on the CPTPP's provisions, thereby offering a focal point for any WTO agreement.

The analysis shows that, ultimately, these provisions do little to promote trade in digital goods and services by ensuring the free flow of data across borders. Conversely, they do not guarantee that member states have the necessary flexibility to regulate data effectively at the national level either. This is because it will be left to state-to-state dispute settlement panels to resolve the uncertainty surrounding the scope of national data regulations. Panels could decide to impose limits on countries' ability to protect their citizens in favour of ensuring unfettered cross-border data flows. There is a risk, however, that such decisions could severely undermine the legitimacy and political support for trade agreements, at least as they pertain to digital trade. Therefore, without proper benchmarks (i.e. internationally agreed standards) for determining what regulatory measures are legitimate to protect consumers, personal information (privacy) and national security, panel members could end up adopting a cautionary approach to judging national data regulations as unreasonable, unnecessary or illegitimate with respect to the

barriers that they impose on cross-border digital trade.[6] Obviously, this assumes that parties to a trade agreement will want to initiate a case under the agreement's dispute settlement mechanism in the first place. Given the uncertainty created by the agreement's digital trade provisions, they may prefer to leave things as they are – better the devil you know than the one you don't know.[7]

CPTPP

The CPTPP contains several provisions in its Chapter 14 (on electronic commerce) that concern data flows. Chapter 14 does not specify what types of data are covered, except to say those that are necessary for business purposes. It also preserves member states' ability to limit the free flow of data held by government entities. The CPTPP also encourages interoperability between data privacy regimes and encourages cooperation between consumer protection authorities.

Consistent with the WTO's waiver on customs duties on electronic commerce, the CPTPP's Article 14.3 prohibits the imposition of customs duties on electronic transmissions; however, it allows "internal taxes, fees or other charges" as long as they are not discriminatory (i.e. applied equally to national as well as foreign entities).

The CPTPP's Article 14.8 mandates a personal data protection floor. Paragraph 2 states: "To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies." Paragraph 3 adds further: "Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction." So, the provisions aim to ensure that signatories have laws and regulations that provide a minimum level of personal information protection; however, they are very flexible in terms of accommodating different national approaches. The fact that paragraph 3 does not oblige parties "to adopt non-discriminatory practices", but simply encourages them to do so – using the hortatory terminology of "shall endeavour" – is potentially problematic for the free flow of personal data across member states' borders and, thus, digital trade between them. The call in paragraph 2 for the parties "to take into account principles and guidelines of relevant international bodies" is a well-established approach in trade agreements; however, there do not exist internationally recognised standards for personal data protection developed

6 Even if international standards existed, there is no guarantee that a dispute settlement panel would base its decision on them. As Mitchell et al. (2016) point out, in the WTO's ***Argentina – Financial Services*** dispute, the "[p]anel declined to assess those reasons based on international standards, specifically noting that 'GATS does not seek to identify measures that could be characterized as specifically prudential. . . such as the Basel Committee'" (p. 810).

7 The same logic might explain why it took seven decades before the national security provision in the GATT (Article XXI) was subject to a (dispute settlement) panel decision, in a case involving Russia and Ukraine (Lacerda Prazeres 2020). It is also noteworthy that there has only been one WTO dispute where the prudential carve-out with respect to trade in financial services has been invoked (Cantore 2018).

by a coherent set of international bodies. And even if such internationally recognised standards and bodies existed, the parties are not obligated to follow them because of, again, the use of hortatory terminology "should take into account" rather than "shall take into account".

The CPTPP's Articles 14.11 and 14.13 prohibit restrictions on cross-border data transfers for business purposes and requirements to localise the storage of data domestically, respectively. However, both articles allow parties to impose such restrictions in pursuit of a "legitimate public policy objective". So, it raises the key question of what a "legitimate" public policy objective is. Article 14.11, paragraph 3 clarifies that a measure restricting cross-border data transfers cannot: (a) be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade"; and (b) "impose restrictions on transfers of information greater than are required to achieve the objective". Article 14.13, paragraph 3 offers the same limitations for restrictions on the use or location of computing facilities. This means that in order to be legitimate, restrictions on cross-border data flows to protect, for example, individuals' privacy must apply indiscriminately to domestic as well as to foreign firms (i.e. the national treatment principle). In other words, restrictive measures cannot be disguised protectionism that favours one or a set of domestic firms at the expense of their foreign competitors. Furthermore, any restriction on cross-border data transfers must be commensurate with the objective that it is meant to achieve; it cannot be stronger or more encompassing that what is strictly required to be effective (i.e. the necessity test).

There are thus limits on the restrictions to cross-border data flows, and in turn digital trade, that the CPTPP's members can impose legitimately. Because the General Agreement on Trade in Services' (GATS) Article XIV provides the basis for the general exception found in provisions such as CPTPP's Articles 14.11 and 14.13, Mitchell and Mishra (2018) argue that "these exceptions may be unable to address all aspects of data flow restrictions" (p. 1095). Given the limited scope of the GATS Articles XIV, many types of restrictions may not be deemed legitimate. For instance, Creach (2019) doubts that data localisation requirements are justifiable because of "the stringent conditions for trade restrictions to fall within the scope of GATS Article XIV (especially the necessity test)" (p. 2). As such, in principle, this is good news for the free flow of data across borders.

Nevertheless, there remains a fair amount of ambiguity as to the extent to which governments can negatively affect digital trade between CPTPP member states by imposing restrictions on data transfers between countries. Ultimately, it would be left to the CPTPP's state-to-state dispute settlement mechanism (DSM) to decide. And, given the absence of internationally agreed regulatory standards, then the basis for a DSM panel decision would be uncertain. As a result, it is entirely possible that parties would refrain from launching a dispute over the adoption of restrictive measures to cross-border flows since a government may not want to set a precedent where a panel of three people gets to decide what is acceptable and what is not when it comes to national data regulation. Such a situation could reduce the CPTPP's legitimacy in the eyes of the public, at least

with respect to its digital trade provisions.[8] The upshot is that the CPTPP's Articles 14.11 and 14.13, despite their stated limits on cross-border data flow restrictions, could possibly not prevent member states from adopting national data regulations that impose serious obstacles to trade in digital goods and services.

USMCA

The CPTPP's Chapter 14 served as the basis for the USMCA's Chapter 19 on "digital trade". The latter terminology, as opposed to "e-commerce" in the CPTPP's case, reflects the chapter's slightly broader scope. As such, the USMCA introduces some differences from the CPTPP with respect to provisions touching on cross-border data flows.

One difference concerns the requirement for USMCA parties to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade" (Article 19.8, paragraph 2). The USMCA goes a bit further than the CPTPP by mentioning explicitly the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as "principles and guidelines of relevant international bodies" when developing a legal framework for protecting personal information.[9] It is, however, doubtful that specifying the APEC Framework and the OECD Guidelines, when compared to the CPTPP, puts additional constraints on member states. This is because the parties to the USMCA, as with the CPTPP, are not required to take into account principles and guidelines of relevant international bodies; they are only encouraged to do so. Unlike the CPTPP, the USMCA also explicitly mentions "key principles" that member states should recognise as they develop their legal framework;[10] however, "principles" is a misnomer here as they are more akin to themes or general categories.

In addition, the USMCA stipulates that the parties "recognize the importance of… ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented" (Article 19.8, paragraph 3), thereby providing some limit on the extent to which data protection legislation or regulation can constrain the transfer of (personal) data between the member states. Such a standard for potentially restricting data flows in order to protect personal information is not present in the CPTPP's Article 14.8, paragraph 2. Nevertheless, it still leaves open the question of determining if and to what extent restrictions are "necessary and proportionate". For example, would a requirement for private organisations in Canada to obtain explicit

8 There is a potential parallel to be made here with the national security exceptions in the GATT and the GATS, in that, as Yoo and Ahn (2016) write, "[t]he all-embracing and seemingly omnipotent Security Exceptions in Article XXI [GATT] has, in effect, been largely conceived throughout the GATT/WTO history for being inapplicable due to its ambiguity and the lack of objective standards to determine whether a measure has been adopted with a view to protecting 'essential security interests'" (p. 426); see also Lacerda Pazeres (2020).

9 The APEC Framework is modelled on the OECD Guidelines.

10 The USMCA's Article 19.8, paragraph 3 states: "The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability".

consent from individuals before the latter's data is transferred across the border to the United States be deemed necessary and proportionate? As with the CPTPP, answering such question would presumably be left to a panel under the USMCA's Chapter 31 (dispute settlement). Again, it would not be the most democratically legitimate way to decide on national data regulation.

There is also a difference between the USMCA and the CPTPP with respect to the provisions on data localisation ("Location of Computing Facilities"). Unlike the CPTPP's Article 14.13, the USMCA's Article 19.12 does not allow the parties to invoke a "legitimate public policy objective" exception to impose a data localisation requirement to firms from the other two parties as a condition for providing a digital good or service in the territory. The only exception possible here is for the specific case when a digital good or service is provided to a government, because the USMCA's Chapter 19 does not apply to government procurement (as is the case with the CPTPP). In other words, governments can only require organisations that collect, hold or process information to locate their computing facilities in the territory when these activities are undertaken for or on behalf of a government. As such, the USMCA is better for ensuring cross-border data flows than the CPTPP.

A final important difference between the USMCA and the CPTPP is the former's Article 19.17 on "Interactive Computer Services", which has no equivalent in the CPTPP. According to this article, internet service providers, social media platforms and search engines, for example, cannot be treated as information content providers for liability purposes, which means that they are not legally responsible for the content generated by users.[11] Presumably, this article prevents member-state governments from regulating user-generated content, such as disinformation for instance, that is found and circulates on such interactive computer services; however, the USMCA stipulates in Annex 19-A that the agreement's general exceptions (e.g. for public morals) applies to Article 19.17. So, once again, we are faced with a situation of uncertainty as to this article's scope of application, which is ultimately left to the USMCA's state-to-state dispute settlement mechanism to address at some point in the future (assuming that one of the parties would want to undertake a dispute).

RCEP

Like the USMCA, the RCEP's Chapter 12 on electronic commerce uses the CPTPP's Chapter 14 as a template. Both chapters have similar language with respect to cooperation, paperless trading, electronic authentication and electronic signature, online consumer protection, personal information protection, unsolicited commercial electronic messages, domestic regulatory framework, customs duties and cybersecurity.

11 The USMCA's provision is based on Section 230 of the US Communications Decency Act.

The RCEP and the CPTPP diverge on provisions covering the location of computing facilities, cross-border transfer of information by electronic means, source code and dispute settlement. In all these cases, the RCEP's Chapter 12 is much weaker than CPTPP's Chapter 14, to the point of rendering the provisions meaningless in terms of liberalising cross-border digital trade and data flows. RCEP's language is such that it allows member states to impose whatever national regulatory restrictions they wish, as long as they are applied in a non-discriminatory way.

But even with respect to the non-discrimination provisions, a member state could get away with discriminating against specific foreign firms since the RCEP's state-to-state dispute settlement mechanism does not apply to Chapter 12, unlike with the CPTPP and the USMCA. If the RCEP's member states cannot resolve a dispute on their own through consultation, then it moves to the RCEP Joint Committee (ministerial level) for further discussion but without the power to impose any decision.

For instance, RCEP's Article 12.14 on the location of computing facilities is almost a mirror image of the first three paragraphs of the CPTPP's corresponding article, but they diverge with the RCEP's addition of a footnote to provision 12.14.3(a): "For the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party". This means that the legitimacy of any public policy that could require a firm to locate computing facilities in a member state is self-judging. In other words, anything can be deemed legitimate if a party says so. And, just in case the footnote is not enough, subparagraph (b) carries on saying that the article does not prevent a party from taking "any measure that it considers necessary for the protection of its essential security interests [...] Such measures shall not be disputed by other Parties". The situation is the same for the RCEP's Article 12.15 on the cross-border transfer of information by electronic means, which has the same language as Article 12.14.

In sum, RCEP's e-commerce (i.e. digital trade) chapter is built on the CPTPP framework, which is not surprising given that many CPTPP member states are also members of the RCEP. However, the RCEP adds and removes language in order to give its member states all the leeway they need to adopt measures restrictive to digital trade and data flows, should they wish to do so. We can only presume that China, which tightly protects its digital realm from the outside world, is behind such weakening language in order to protect its 'Great Firewall'.[12]

12 For a description of China's digital realm in comparison with those of the EU and the US, see Aaronson and Leblond (2018).

WTO

The RCEP's Chapter 12 on electronic commerce is probably a good harbinger of the kind of agreement that we can expect at the WTO's Joint Statement Initiative (JSI) on Electronic Commerce, which aims to negotiate a plurilateral agreement on "trade-related aspects of electronic commerce".[13] This is because it showcases what China – the RCEP's dominant member state – is willing to accept in terms of e-commerce/digital trade provisions. Given existing divisions among WTO members regarding e-commerce/digital trade negotiations (Aaronson and Struett 2020), it is reasonable to assume that the Chinese government is unlikely to accept language that would constrain its ability to control the type of data as well as the type of digital goods and services that goes in and out of China (Aaronson and Leblond 2018, Gao 2018). As such, the WTO's plurilateral agreement is likely to reflect the lowest common denominator positions if it is ever to be finalised.

The JSI process began at the WTO's ministerial conference in Buenos Aires in December 2017, when some 75 members issued a joint statement that "recognize[d] the important role of the WTO in promoting open, transparent, non-discriminatory and predictable regulatory environments in facilitating electronic commerce".[14] As with the CPTPP, the USMCA and the RCEP, the recently leaked JSI consolidated negotiating text (see discussion below), dated December 2020, falls short of such lofty objectives.

JSI negotiations began in 2018 to delimit the scope of potential plurilateral negotiations on electronic commerce/digital trade. In April 2019, the key players in the negotiations – China, the European Union and the United States – issued their proposals to the WTO's plurilateral negotiations on trade-related aspects of electronic commerce. These proposals occupied different places on a continuum that includes independent national data protection at one end and free cross-border data flow at the other (Leblond 2021). China is close to the former pole and the United States is close to the latter pole, with the EU in between.[15]

In February 2021, the JSI's consolidated negotiating text was leaked.[16] According to the text, several members "expect security, general and prudential exceptions to apply" (p. 1). Several members have also indicated that their commitments would not apply to government procurement and information held or collected by or on behalf of government as well as financial services.

Overall, the JSI's consolidated negotiating text confirms that Canada, Japan and the United States are, not surprisingly, pushing for the CPTPP's language with regards to provisions affecting the transfer of data between the parties. On cross-border data flows (p. 27), there appears to be a general agreement among the parties that they shall allow

13 Aaronson and Struett (2020) provide a short history of WTO negotiations on e-commerce/digital trade.
14 "Joint statement on Electronic Commerce," WT/MIN(17)/60, 13 December 2017 (www.wto.org/english/thewto_e/minist_e/mc11_e/documents_e.htm).
15 The European Union stands in between the Chinese and US poles mostly because it seeks no limits on its ability to protect personal data.
16 www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf.

(or not prohibit) the "transfer of information by electronic means" for business purposes (para. 5). However, there is also language that protects the parties' ability to adopt or maintain measures inconsistent with paragraph 5 to achieve a legitimate public policy objective (para. 6). Here, we find the CPTPP's language (found in Article 14.11) in that such measures be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade" and do not "impose restrictions on transfers of information greater than are required to achieve the objective". The European Union goes even further by proposing what essentially amounts to a full exception to the prohibition on restricting cross-border flows when it comes to protecting personal data and privacy.

Notwithstanding the European Union's additional language to limit the transfer of personal data across border, the consolidated negotiating text contains separate provisions (p. 45) – like in the CPTPP, USMCA and RCEP – to the effect that the parties "recognise" the benefits or importance of protecting personal data and privacy and that they shall take into account the principles and guidelines/international standards of relevant international bodies (such as the OECD).

As with the CPTPP's Article 14.13, the WTO negotiating text contains provisions to prohibit data localisation. In the section on "location of computing facilities" (p. 30), the text indicates that a member shall not require the use or location of facilities in that member's territory as a condition of doing business in that territory. However, following the CPTPP, the text continues with provisions stating that the parties cannot be prevented from adopting or maintaining measures contrary to the above-mentioned prohibition in order to pursue a legitimate public policy objective, as they are "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade" and do not "impose restrictions on transfers of information greater than are required to achieve the objective".

The consolidated negotiating text also includes, following the United States' proposal, the USMCA's (Article 19.17) provisions that limit the legal liability of interactive computer services (p. 24). For its part, according to the negotiating text, China has not proposed language with respect to cross-border data flows and the location of computing facilities. Given that the Chinese government has requirements on the latter as a condition of doing business in its territory while it imposes clear restrictions on the former (Aaronson and Leblond 2018), one would have expected the additional RCEP language to find itself in the consolidated negotiation text. Or, perhaps, it simply reflects the fact that, in China's spring 2019 submission to the WTO negotiations, Article 4.2 stated that issues such as data flows and data storage require "more exploratory discussions [...] before bringing [them] to the WTO negotiation" (Leblond 2021). Interestingly, and in line with the RCEP's additional weakening language when compared to the CPTPP with respect to cross-border data flows and the location of computing services, China's WTO submission also included the following (Article 4.3): "the data flow [sic] should be subject to the precondition of security, which concerns each and every Members' core interests. To this end, it is necessary that

the data flow orderly [sic] in compliance with Members' respective laws and regulations" (Leblond 2021). This would explain why, as per the consolidated negotiation text, China has proposed to enlarge the scope of Article XIV bis of the GATS on the security exception (p. 86). China's proposal is identical to the GATS article, except that it removes the three conditions that specify the scope of the article's applicability.[17] As result, in principle, any measure to limit the cross-border flow of data and digital trade would be acceptable if a member claims that the measure is necessary to protect its national security.

In sum, when compared to the CPTPP, the USMCA and the RCEP, the above analysis of the WTO's consolidated negotiation text suggests that an agreement on "trade-related aspects of electronic commerce" is highly unlikely to contain stronger language to prevent member states from imposing barriers to digital trade through national regulations that control or limit cross-border data flows. Thus, if it ever comes about, the agreement will fail in achieving its stated objective of providing its members with "predictable regulatory environments in facilitating electronic commerce". As seen also in this section, the same conclusion applies to the CPTPP, the USMCA and, even more so, the RCEP.

GOVERNING CROSS-BORDER DATA FLOWS: DRAWING INSPIRATION FROM INTERNATIONAL FINANCE'S REGULATORY ARCHITECTURE

The analysis undertaken in the previous section makes clear that existing trade agreements are, on their own, ineffective instruments to facilitate international trade in digital goods and services through the free flow of data across borders. Given the growing importance of data-driven markets and their effects on individuals, society and economy in terms of, for example, privacy, competition, democracy, public safety and national security, it cannot reasonably be left to a few people on dispute settlement panels to decide what are 'legitimate public policy objectives' and 'necessary and appropriate' measures that parties to a trade agreement can pursue with respect to regulating their national data-driven markets. Such an approach makes even less sense considering that there are no internationally accepted standards on which to base such decisions. As a result, member states are likely to refrain from launching disputes on digital trade matters, as they have done with the national security exception and the prudential carve-out for financial services. So, the digital trade provisions in trade agreements would end up being useless to all intents and purposes. Following the data trilemma's logic, cross-border data flows and, thus, digital trade would likely suffer, because member states would face no constraints as they regulate data-driven markets to increase trust amongst

17 Article XIV bis of the GATS states: "Nothing in this Agreement shall be construed: (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests: (i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment; (ii) relating to fissionable and fusionable materials or the materials from which they are derived; (iii) taken in time of war or other emergency in international relations". China's proposal in the consolidated negotiation text reads: "Nothing in this Agreement shall be construed: (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests".

consumers, businesses and governments. Such a scenario would not only hurt innovation and competition, it would also increase the digital divide between countries (Aaronson 2019b, Aaronson and Leblond 2018).

In order to avoid this scenario and, instead, achieve the 'free cross-border data flows with trust' axis on the data trilemma, Leblond and Aaronson (2019) put forward the idea of a single data area that would be developed outside trade agreements. According to the authors, an effective single data area would allow personal and non-personal data to flow freely between the member states' borders, because those who use, produce, trade, store and process this data would be equally well protected everywhere within the area by common (or equivalent) high-quality data regulations and standards. This type of single data area would welcome and support (financially and technically) any country willing to adopt and enforce the common regulatory standards, which would help address the fact that a large number of countries, including industrialised ones, "are struggling to govern the many different types and uses of data" (Aaronson 2019b). As such, the envisaged single data area would go much further than digital/data rights-based conventions and principles such as the Council of Europe's Convention 108+ or the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

According to Leblond and Aaronson (2019), an international body would need to be responsible for setting standards that regulate the creation, processing, use, distribution and transfer of data, both personal and non-personal, within the single data area. It would also have to be responsible for monitoring that the states that are members of the single data area apply and enforce the common standards adequately. This organisation's frequent assessments would determine whether or not a member state is able to continue taking full part in the single data area.[18] In case of inadequate application or enforcement, the other members of the single data area would be allowed to restrict data flows to a member state that is not in good standing until proper actions have been taken to remedy the situation.

International financial standard-setting bodies

After reviewing proposals for a WTO 2.0 (Ciuriak 2019) or the IMF (Balsillie 2019) to take on this data standard-setting responsibility, Leblond and Aaronson (2019) conclude that existing international organisations do not have the required expertise to do so and that, as a result, a new international body should be created. Fay (2019) argues that this new international body should be modelled after the Financial Stability Board (FSB), which coordinates, under a G20 remit, a number of international financial standard-setting bodies to ensure the global financial system's stability. Fay proposes a 'digital stability

18 Restrictions on participating in the single data area could be limited to the type of data where standards are not being applied or enforced properly.

board' that would "take its mandate from global leaders and coordinate work on global principles and standards for the big data and AI realm, while working with domestic agencies responsible for data and AI policy to best reflect national values and customs".

In pursuit of Leblond and Aaronson's (2019) vision for a single data area, a digital stability board modelled on the FSB may not be the most effective design for a new international organisation to set and enforce standards for data-driven markets. With its small staff (mostly on loan from national governments or international financial institutions), the FSB acts as a coordinating and information exchange body for its member states' financial authorities, international financial institutions (the IMF, the World Bank and the Bank for International Settlements) and international financial standard-setting bodies such as the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, the International Association of Insurance Supervisors and the International Accounting Standards Board. On its website, the FSB describes its mandate as follows: "The FSB promotes international financial stability; it does so by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies. It fosters a level playing field by encouraging coherent implementation of these policies across sectors and jurisdictions".[19] The FSB ultimately reports to G20 leaders (heads of states and governments), which gives it authority on the one hand but limits its autonomy and discretion on the other (Helleiner 2010, Moschella 2013).

Rather than the FSB that coordinates them, standard-setting bodies (SSBs) such as the Basel Committee on Banking Supervision, the International Organisation of Securities Commissions and the International Accounting Standards Board represent better models for a new international regulatory body to govern cross-border data flows. They devise the principles, norms and standards that serve as accepted best practices for governing financial activities. These SSBs are also more removed from political interference since they are often governed by national regulators, which tend to have significant degrees of autonomy from governments and politicians as a result of the technical nature of their work (Roger 2020: 165). Combined with their less formal nature, this allows these SSBs to respond more rapidly to changes occurring in financial markets (Brummer 2010). The key to their success is that they are "guided by a stable of skilled technocrats who develop shared expectations and trust allowing them to dispense with time-consuming treaties and formal international organizations" (Brummer 2010: 634). Moreover, their effectiveness depends on their decisions being perceived as neutral, which requires that all relevant experts and stakeholders have been included in the decision-making process (Kerwer 2005).[20]

19 www.fsb.org/about/#mandate.

20 Brummer (2010: 642) notes that many of these SSBs are 'exclusive' clubs (traditionally of regulators from wealthy countries), which export their rules to the rest of the world. As a result, they "can be exposed to charges of being unrepresentative [...] and lacking in transparency and accountability".

Recognised expertise and neutrality are important because the financial regulatory principles and standards developed by the SSBs are not binding on the national regulators that participate in their development. The decisions of SSBs are thus 'soft law', which is "obeyed in a voluntary and self-imposed way" as opposed to the "coercive and externally imposed way" that applies to 'hard law' (Peihani 2015: 148). Brummer (2010) argues that national regulatory authorities adopt and implement SSBs' non-binding standards because they want to remain part of the 'club' and not be considered as 'second-class citizens' or face suspension (or even expulsion) in their membership if they fail to comply with agreed-upon standards. In addition, he observes that "[s]haming can also, importantly, carry costs beyond institutional and professional reputations: [b]y publicly identifying jurisdictions that do not comply with their standards, institutions can create new market costs by implying or arguing that non-cooperative jurisdictions suffer from poor domestic oversight and market supervision and thus are somehow risky or dishonorable places to do business" (p. 641).

The Basel Committee on Banking Supervision (BCBS), created in 1974, is the oldest international financial SSB. Like most other SSBs, it is a transgovernmental network of central bankers and banking supervisors from G20 members as well as Hong Kong and Singapore that is housed in the Bank for International Settlements, which provides it with a 17-person secretariat (Peihani 2015: 148). It was created as a "forum for cooperation on banking supervisory matters and as a global standard setter in prudential regulation" (quoted in Milano and Zugliani 2019: 165). The Committee has no legal personality or formal regulatory authority and, as a result, its decisions have no legal force. As mentioned above with respect to SSBs in general, it relies on reputational and market costs as well as other sanctioning mechanisms to ensure compliance with its decisions, which require consensus among members. According to Milano and Zugliani (2019), "[i]nformality and consensual regulation, together with increasing transparency and participation of stakeholders, ensure effectiveness, endogenous legitimacy, and flexibility in a highly technical and evolving field of regulation" (p. 175). The Committee is organised into five standard-setting and research-based groups: policy development, supervision and implementation, macroprudential supervision, accounting experts and Basel consultative.[21] Each group contains working groups, which are responsible for specified technical work, and task forces, which undertake specific tasks for a limited time. The Policy Development Group (PDG) develops "policies that promote a sound banking system and high supervisory standards". The Supervision and Implementation Group fosters "the timely, consistent and effective implementation of the Basel Committee's standards and guidelines; and [...] advances improvements in banking supervision, particularly across Basel Committee members". The Macroprudential Supervision Group (MPG) "monitors systemic risk and global developments that relate to macroprudential and systemically important bank (SIB) supervision and [...] provides guidance to other groups working on

21 www.bis.org/bcbs/organ_and_gov.htm.

issues related to macroprudential/SIB supervision, and develops specific policy proposals, as needed, to fill gaps, address inconsistencies or tackle unintended consequences in the overall framework of macroprudential/SIB supervision". The Accounting Experts Group (AEG) "helps ensure high quality international accounting standards and practices [as well as] high quality audit and ethics standards and practices for auditors". Finally, The Basel Consultative Group (BCG) "provides a forum [that] facilitates broad supervisory dialogue with non-member countries on new Committee initiatives early in the process by gathering senior representatives from various countries, international institutions and regional groups of banking supervisors that are not members of the Committee". Peihani (2015) finds that the Committee has "become increasingly more accountable since its inception" (p. 157). He says that it now discloses more information on how it operates and develops policies, even if it could be even more transparent. The Committee has also increased its engagement with stakeholders through a 'notice and comment' process in the development of standards,[22] although Peihani notes that more effort could be done to involve stakeholders beyond the financial industry (e.g. consumers, retails investors and non-governmental organisations) (see also Riepe 2019: 269 and Viterbo 2019: 228).

The International Organisation of Securities Commissions (IOSCO), created in 1983, is a regulatory network of financial supervisors, like the BCBS, but for securities markets rather than banking. It is based in Madrid and supported by a secretariat with more than 30 people. Its membership comprises 130 jurisdictions that cover more than 95% of the world's securities markets.[23] It is "devoted to promoting common and efficient regulations, setting the floor for the exchange of information between its members, improving the effective surveillance of international securities transactions, and increasing the mutual assistance necessary for the integrity of global financial markets" (Marcacci 2012: 23). The IOSCO has three categories of members: ordinary, associate and affiliate.[24] The IOSCO Board is the IOSCO's governing and standard-setting body, with 34 securities regulators belonging to it (based on market size). The IOSCO Board conducts its policy work through eight committees: issuer accounting, auditing and disclosure; regulation of secondary markets; regulation of market intermediaries; enforcement and the exchange of information and the Multilateral Memorandum of Understanding Screening Group; investment management; credit rating agencies; commodities derivatives markets; and retail investors.[25] The IOSCO Board also relies on input from the Growth and Emerging

22 Riepe (2019) describes the Committee's notice and comment process as follows: "New regulatory ideas and potential measures are first communicated to the stakeholders in the form of consultative papers; and all parties, especially banks and banking associations but also other interested parties such as the IASB, are invited to express their opinions in the form of a comment letter" (p. 267).

23 www.iosco.org/about/?subsection=about_iosco.

24 "In general, the ordinary members (129) are the national securities commissions or similar governmental bodies with significant authority over securities or derivatives markets in their respective jurisdictions. Associate members (33) are usually supranational governmental regulators, subnational governmental regulators, intergovernmental international organizations and other international standard-setting bodies, as well as other governmental bodies with an appropriate interest in securities regulation. Affiliate members (67) are self-regulatory organizations, securities exchanges, financial market infrastructures, international bodies other than governmental organizations with an appropriate interest in securities regulation, investor protection funds and compensation funds, and other bodies with an appropriate interest in securities regulation" (www.iosco.org/about/?subsection=about_iosco).

25 www.iosco.org/about/?subsection=display_committee&cmtid=11.

Markets Committee (comprising 91 members and 22 non-voting associate members)[26] four regional committees (Africa/Middle East, Asia-Pacific, European, Inter-American) and the Affiliate Members Consultative Committee.[27] The IOSCO Board reports to the Presidents' Committee, which meets once a year and is composed of all the presidents/chairs of IOSCO's ordinary and associate members. According to Marcacci (2012), the Presidents' Committee "is responsible for adopting the resolutions that reformulate IOSCO's mission and goals, setting up the Organisation's operational priorities, amending the by-laws, admitting new members, recognizing the regional committees, determining the annual contribution for the members, and imposing sanctions upon members" (p. 29). It is also responsible for nominating members to the IOSCO Board. It is noteworthy that the IOSCO's By-Laws include three types of sanction: "suspension of a member's voting rights for a certain period; the suspension of a member from membership in the Organisation for a certain period; and the exclusion of a member from membership" (Marcacci 2012: 35). To evaluate members' implementation of the IOSCO's standards and policies, an Assessment Committee, reporting to the IOSCO Board, was set up in early 2012.[28]

In 2002, the IOSCO adopted the Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU), which "represents a common understanding among its signatories of how they should consult, cooperate, and exchange information for the purpose of regulatory enforcement regarding securities markets".[29] According to Austin (2015), the MMoU has been used as a lever to effect changes in signatories' domestic legislation and, therefore, bring about more international convergence in securities regulation. Leverage has been achieved in two, complementary ways. First, MMoU applicants have to undergo a "thorough and demanding screening process", whereby they are assessed to ensure that "they have the laws in place which would allow them to exchange required information and comply with the MMoU" (Austin 2015: 12). Second, it adopted measures to help and encourage non-signatory members to apply to join the MMoU. For instance, in June 2010, IOSCO's Presidents Committee adopted a resolution for the creation of a 'watch list' of the members that had not applied to become part of the MMoU by January 1, 2013. Two years later, it adopted another resolution for IOSCO to set up a programme of technical assistance and political support for non-signatory members in order to help them make the necessary changes to their legal system. It also considered limiting non-signatory members' participation in

26 "The GEM seeks to promote the development and greater efficiency of emerging securities and futures markets by establishing principles and minimum standards, providing training programs and technical assistance for members and facilitating the exchange of information and transfer of technology and expertise" (www.iosco.org/about/?subsection=display_committee&cmtid=8).

27 "The AMCC objectives are to share experiences and enhance cooperation among its members. In its capacity as a consultative committee, it provides input into the IOSCO policy and standard-setting work. The AMCC also has its own streams of work, including the Regulatory Affairs Group, the Emerging Risks Group and the Regulatory Staff Training Working Group, which organizes every year the AMCC Training Seminar on Implementing IOSCO Principles. The AMCC establishes Task Forces to investigate topics with specific relevance for AMCC members and/or the broader IOSCO community" (www.iosco.org/about/?subsection=display_committee&cmtid=2).

28 www.iosco.org/about/?subsection=display_committee&cmtid=19.

29 www.iosco.org/about/?subsection=mmou.

IOSCO decision making, which it subsequently did when signing onto the MMoU became a condition of membership. As a result, non-signatory members lost their voting rights, could no longer nominate candidates for election or appointment to leadership positions within IOSCO, and were suspended from participating in committees and task forces. In 2016, IOSCO adopted the Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (EMMoU), which is to replace the MMoU with additional 'key powers' necessary "to ensure continued effectiveness in safeguarding market integrity and stability, protecting investors and deterring misconduct and fraud include".[30]

The International Accounting Standards Board (IASB), created in 2001, is a London-based private international organisation that sets international financial reporting standards. It emerged out of the International Accounting Standards Committee (founded in 1973) in order to become "the primary international standard setter" for financial reporting rather than simply try to harmonise accounting standards throughout the world (Ruder et al. 2005: 528). According to the IFRS Foundation, which governs the IASB, out of 166 countries analysed, there are currently 144 jurisdictions that "require IFRS Standards for all or most domestic publicly accountable entities (listed companies and financial institutions) in their capital markets".[31] The IASB's standard-setting process is underpinned by two key principles in order to ensure high-quality standards: independence and transparency. From the beginning, the IASB has emphasised that it does not represent the interests of a particular country or group of countries but those of the world's capital markets; it has portrayed itself as a technical body that is "insulated from national political pressures" (Tweedie and Seidenstein 2005: 595). Notwithstanding the pressures exercised over it by the European Union and the United States during its first years of existence, the IASB managed to maintain its independent nature (Leblond 2011). The IASB ensures its independence and neutrality in three ways. First, its staff members are hired for their relevant expertise in matters of financial reporting standards.[32] In 2019, the IFRS Foundation and IASB counted on the support of 150 staff members. Second, it follows a 'due process' through which it issues a preliminary version of a proposed standard (called an 'exposure draft') to the public and asks for comments and feedback before issuing the standard's final version (IFRS Foundation 2020). Finally, as a private international organisation, it is not beholden to national governments for its existence (as it is directly governed by a non-profit private foundation, the IFRS Foundation).[33] Nevertheless, in February 2009, the IFRS Foundation set up the Monitoring Board in order to boost its

30 www.iosco.org/about/?subsection=emmou.

31 www.ifrs.org/use-around-the-world/use-of-ifrs-standards-by-jurisdiction/#analysis.

32 In 2012, according to Leblond (2011: 455), the IFRS Foundation expanded the Board's members from 14 to 16 with a recommended geographical distribution, which did not exist before: four members from Asia/Oceania; four members from Europe; four members from North America; one member from Africa; one member from South America; and two members appointed from any area (subject to maintaining overall geographical balance).

33 The Trustees of the IFRS Foundation "are responsible for the governance and oversight of the IFRS Foundation and the International Accounting Standards Board. The Trustees are not involved in any technical matters relating to IFRS Standards. This responsibility rests solely with the Board. The Trustees are accountable to the Monitoring Board, a body of publicly accountable market authorities" (www.ifrs.org/groups/trustees-of-the-ifrs-foundation/).

legitimacy in terms of public accountability. The Monitoring Board is responsible for ensuring that "the Trustees continue to discharge their duties as defined by the IFRS Foundation Constitution, as well as approving the appointment or reappointment of Trustees".[34] It meets once a year, or more if necessary, and consists of representatives from the European Commission, the US Securities & Exchange Commission, Japan's Financial Services Agency, China's Ministry of Finance, Korea's Financial Services Commission, Brazil's Comissão de Valores Mobiliário, the IOSCO Board, and the IOSCO's Growth and Emerging Markets Committee. Representatives from the BCBS (Chair of the Accounting Experts Group) and IOSCO's European Regional Committee also participate as observers. As a result, "securities regulators that allow or require the use of IFRS in their jurisdictions [are] able to more effectively carry out their mandates regarding investor protection, market integrity, and capital formation".[35] The IASB relies on a number of consultative bodies, representing different stakeholder groups, to advise it.[36] According to recent a study by Hewa et al. (2020), the IASB manages to maintain its independence while it obtains valuable input from stakeholders through its 'due process'.

In sum, financial standard-setting bodies like the Basel Committee on Banking Supervision, the International Organisation of Securities Commissions and the International Accounting Standards Board have developed elaborate governance structures to ensure that their standards are adopted widely around the world. Their standards' legitimacy and acceptance depend not only on recognised technical expertise but also on transparent and inclusive due processes that effectively take into account the views of all relevant stakeholders while minimising political interference. These SSBs mostly rely on reputational and market pressures for the adoption and effective implementation of their standards, although formal sanctioning mechanisms are also used in some instances (e.g. IOSCO).

International Data Standards Board

To allow 'data free flow with trust'[37] within a single data area, we need an international body to develop high-quality standards and enforce their effective implementation by member states. Such a body does not currently exist. As discussed above, existing international organisations, such as the IMF and the WTO, are not well suited to take on such tasks. Therefore, a new international standard-setting body should be created. In order to rapidly gain legitimacy and members, this body should be built by drawing the best features from the three financial SSBs discussed in the previous section: the IASB, the BCBS and IOSCO. Given that its creation would not be based on an international treaty negotiated by states but on a more informal transgovernmental network structure adopted by the BCBS and IOSCO, this new body's name should not contain the word

34 www.ifrs.org/groups/ifrs-foundation-monitoring-board/.
35 ibid.
36 www.ifrs.org/about-us/consultative-bodies/.
37 Former Japanese Prime Minister, Abe Shinzo, first introduced this phrase during a speech at the 2019 annual meeting of the World Economic Forum in Davos (Abe 2019).

'organisation' in order to avoid any potential confusion as to its legal nature (as has been the case with IOSCO). As such, the name suggested by Leblond and Aaronson (2019) seems appropriate – the International Data Standards Board (IDSB).

The IDSB would be responsible for devising common principles and standards to ensure a high degree of trust in the data-driven economy among the single data area's individuals, consumers, workers, businesses and governments so that all forms of data could flow freely across borders. It would develop standards on data consent, ownership, collection, processing, aggregation, transmission, storage, analysis, certification and disposal (Girard 2019). To do so, the IDSB would follow the same principles that the above-mentioned financial SSBs espouse: independence, transparency, consensus and broad stakeholder participation. It would have to be flexible enough with sufficient resources (financial, human and technological) to respond effectively and in a timely manner to rapidly evolving digital technologies and markets.

Like with the BCBS and IOSCO, national regulatory authorities would be responsible for implementing the IDSB's decisions. National (or, in the case of the European Union, supranational) data protection authorities or their equivalent would be the logical choice for such a role. Countries that do not have such authorities would have to set them up in order to become members of the IDSB and be able to take part in the single data area. The IDSB would provide extensive financial and technical support to help countries put in place the necessary national data regulation authorities and associated legislations so that they could quickly become IDSB members. In exchange, following IOSCO's governing structure, national data regulation authorities would be responsible for steering the IDSB's work. For instance, there could be a Presidents' (or Chairs') Committee that would meet at least once a year to formulate the IDSB's mission and objectives, set its operational priorities, amend its by-laws, admit new members, sanction existing ones, determine members' annual contributions, and appoint individuals to the IDSB's Executive Committee, which would be responsible for setting data standards (as do the IOSCO Board and the IASB). Each IDSB member would have one vote within the various decision-making committees, sub-committees and working groups.

Appointments to the IDSB's Executive Committee would be based on some accepted measure of the value of members' digital markets or data-dependent economy, in the same way that IOSCO Board members reflect the size of their securities markets. However, Executive Committee membership should also ensure that there is a balanced geographical representation, as is the case with the IASB. Similar to the BCBS's research groups and the IOSCO Board's committees, the Executive Committee's standard-setting and research work would be divided into sub-committees. These sub-committees would handle issues such as protecting individuals' privacy (e.g. consent and data-breach disclosures), conducting certifications and audits, regulating data market intermediaries (e.g. data trusts), ensuring adequate implementation and supervision by members, ensuring enforcement and sharing of information between members (possibly through a multilateral memorandum of understanding similar to the IOSCO's), training and

technical assistance to aspiring members, monitoring emerging technologies, and so on. Like the financial SSBs, the IDSB would put in place a transparent 'due process' for developing standards that are perceived as neutral and legitimate by national data regulators and stakeholders.

Consultative bodies that represent all relevant stakeholders would support the work of the IDSB's sub-committees. It remains unclear at this stage what approach would be best to categorise stakeholders. One approach, for example, could be based on data functions, assuming that they could be organised in some way (e.g. data owners, data collectors, data intermediaries, data storers, data users, data analysts, data auditors, data certifiers, etc.) Another approach could involve national associations representing consumers, workers and businesses (large and small). Representation of economic sectors that rely heavily on data for their activities could be yet another approach to involving stakeholders in the IDSB's decision making. Geographical representation should also be taken into account in organising the IDSB's consultative bodies, perhaps like IOSCO's regional committees. Ultimately, a combination of the above-mentioned approaches would probably be best for ensuring that all relevant stakeholders are properly represented and consulted in the IDBS's decision making.

A permanent secretariat would support the IDSB's work, as with the financial SSBs. As the IDSB would rely on national data protection authorities to provide expert technical staff to participate in sub-committees and working groups, like the BCBS and IOSCO do, it would not need to possess a large permanent technical staff like the IASB has (because national accounting standard-setting bodies only have a consultative role and are not part of the IASB's governance).

Finally, as with the financial SSBs, the IDSB would ensure compliance among its members through a combination of indirect and direct sanctioning. Indirect sanctions would occur through reputational and market pressures as a result of regular, publicly available country assessments. In addition, non-compliant members could face formal or direct sanctions: public warnings, temporary suspension from participating in IDSB activities and decision-making and/or the single data area (for all or only certain types of data) or, ultimately, exclusion from the IDSB and the single data area.

CONCLUSION

Owing to their rapid rise in the last decade or so, cross-border data flows and digital trade are increasingly becoming governed by trade agreements. The most recent instances are the Regional Comprehensive Economic Agreement and the United States–Mexico–Canada Agreement, whose e-commerce/digital trade chapters follow closely that of the Comprehensive and Progressive Agreement on Trans-Pacific Partnership. A plurilateral agreement on 'trade-related aspects of electronic commerce' under the WTO's aegis is also in the works. Unfortunately, such agreements are ineffective instruments to facilitate international trade in digital goods and services through the free flow of data

across borders. Following the data trilemma's logic, digital trade would likely suffer. In one scenario, member states would face few or no constraints from the agreements as they regulate data-driven markets to increase trust amongst consumers, businesses and governments; however, cross-border data flows and, thus, digital trade would face severe restrictions. In the other scenario, member states would be forced to allow the free flow of data across borders as a result of the trade agreements; however, trust in data-driven markets or data-dependent business activities would be negatively affected, which could hurt digital trade.

The governance solution to support international digital trade based on unrestricted cross-border data flows and high levels of trust amongst consumers, businesses and governments lies outside of trade agreements. Building on Leblond and Aaronson (2019), this chapter develops the structural contours of an International Data Standards Board using the model provided by international financial standard-setting bodies such as the Basel Committee on Banking Supervision, the International Organisation of Securities Commissions and the International Accounting Standards Board. Transposing the characteristics of these bodies to a new international data standard-setting body should permit members to allow data to flow freely between them as they would apply the same standards as well as cooperate closely in terms of not only developing the standards but also sharing information and enforcing compliance. As a result, members of the IDSB would form a single data area between them.

A world of emerging digital realms (the main ones being China, the European Union and the United States) that could become incompatible at some point in the future will put increasing pressure on the governments of the countries standing in between these realms to choose one versus another (Aaronson and Leblond 2018). For example, Canada and Mexico would face strong pressure to join the US realm, while Iceland, Norway, the United Kingdom and Switzerland would be attracted to the EU realm. As a result of this fragmentation (what some have called the 'splinternet'), international digital trade and the global economy would suffer. An International Data Standards Board and its accompanying single data area would overcome such fragmentation. Although it takes into account the fact that some members would be better represented than others based on the value of their data-driven economy, it nevertheless treats all members equally in terms of 'one member, one vote' with consensual decision making, transparency, due process, comprehensive stakeholder engagement and geographical balance. If a large number of countries with different economic structures have been able to come together to develop, adopt and implement international financial regulatory standards, then there is no reason why the same could not be achieved for data.

REFERENCES

Aaronson, S A (2019a), "What are we talking about when we talk about digital protectionism?", *World Trade Review* 18(4): 541-577.

Aaronson, S A (2019b), "Data is a development Issue", CIGI Paper No. 223, Centre for International Governance Innovation.

Aaronson, S A and P Leblond (2018), "Another digital divide: The rise of data realms and its implications for the WTO", *Journal of International Economic Law* 21(2): 245–272.

Aaronson, S A and T Struett (2020), "Data is divisive: A history of public communications on e-commerce, 1998-2020", CIGI Paper No. 247, Centre for International Governance Innovation.

Abe, S (2019), "'Defeatism about Japan is now defeated", speech at the World Economic Forum, Davos, 23 January (www.weforum.org/ agenda/2019/01/abe-speech-transcript/).

Austin, J (2015), "The power and influence of IOSCO in formulating and enforcing securities regulations", *Asper Review of International Business and Trade Law* 15: 1-24.

Balsillie, J (2019), "Jim Balsillie: 'Data is not the new oil — it's the new plutonium'", *The Financial Pos*t, 28 May.

Brummer, C (2010), "Why soft law dominates international finance – and not trade", *Journal of International Economic Law* 13(3): 623–643.

Cantore, C M (2018), *The prudential carve-out for financial services: Rationale and practice in the GATS and preferential trade agreements*, Cambridge University Press.

Ciuriak, D (2019), "World Trade Organization 2.0: Reforming multilateral trade rules for the digital age", CIGI Policy Brief No. 152, Centre for International Governance Innovation.

Ciuriak, D and M Ptashkina (2018), "The digital transformation and the transformation of international trade", RTA Exchange, Issue Paper, January, Inter-American Development Bank and International Centre for Trade and Sustainable Development.

Cory, N (2017), "Cross-border data flows: Where are the barriers, and what do they cost?", Information Technology & Innovation Foundation, 1 May.

Creach, M A (2019), "Assessing the legality of data-localization requirements: Before the tribunals or at the negotiating table?", Columbia FDI Perspectives No. 254, Columbia Center for Sustainable Investment.

Fay, R (2019), "The world faces a turning point on data and AI. Will we learn from the financial crisis?", *The Globe and Mail*, 28 May.

Ferracane, M and E van der Marel (2019), "Do data policy restrictions inhibit trade in services?", EUI Working Paper RSCAS 2019/29, Global Governance Programme-342, European University Institute, Robert Schuman Centre for Advanced Studies.

Gao, H (2018), "Digital or trade? The contrasting approaches of China and US to digital trade", *Journal of International Economic Law* 21(2): 297–321.

Girard, M (2019), "Big data analytics need standards to thrive: What standards are and why they matter", CIGI Papers No. 209, Centre for International Governance Innovation.

Helleiner, E (2010), "What role for the new Financial Stability Board? The politics of international standards after the crisis", *Global Policy* 1(3): 282-290.

Hewa, S I, R Mala and J Chen (2020), "IASB's independence in the due process: An examination of interest groups' influence on the development of IFRS 9", *Accounting & Finance* 60: 2585-2615.

IFRS Foundation (2020), "Due process handbook", August.

Kerwer, D (2005), 'Rules that many use: Standards and global regulation', *Governance* 18(4): 611–32.

Knake, R K (2020), "Weaponizing digital trade: Creating a digital trade zone to promote online freedom and cybersecurity", Council Special Report No. 88, Council on Foreign Relations.

Lacerda Prazeres, T (2020), "Trade and national security: Rising risks for the WTO", *World Trade Review* 19: 137–148.

Leblond, P (2011), "EU, US and international accounting standards: A delicate balancing act in governing global finance", *Journal of European Public Policy* 18(3): 443-461.

Leblond, P (2021), "Uploading CPTPP and USMCA provisions to the WTO's digital trade negotiations poses challenges for national data regulation: Example from Canada", forthcoming in M Burri (ed) *Big data and global trade law*, Cambridge University Press.

Leblond, P and S A Aaronson (2019), "A plurilateral 'single data area' is the solution to Canada's data trilemma", CIGI Papers No. 226, Centre for International Governance Innovation.

Marcacci, A (2012), "IOSCO: The world standard setter for globalized financial markets", *Richmond Journal of Global Law and Business* 12(1): 23-44.

McKinsey (2016), "Digital globalization: The new era of global flows", McKinsey Global Institute, March.

Meltzer, J P (2019), "Governing digital trade", *World Trade Review* 18(S1): 523–48.

Milano, E and N Zugliani (2019), "Capturing commitment in informal, soft law instruments: A case study on the Basel Committee", *Journal of International Economic Law* 22: 163–176.

Mitchell, A D, J K Hawkins and N Mishra (2016), "Dear prudence: Allowances under International Trade and Investment Law for Prudential Regulation in the Financial Services Sector", *Journal of International Economic Law* 19: 787–820.

Mitchell, A D and N Mishra (2018) "Data at the docks: Modernizing international trade law for the digital economy", *Vanderbilt Journal of Entertainment & Technology Law* 20: 1073–134.

Moschella, M (2013), "Designing the Financial Stability Board: a theoretical investigation of mandate, discretion, and membership", *Journal of International Relations and Development* 16(3): 380–405.

OECD (2019), "Trade in the digital era", OECD Going Digital Policy Note (www.oecd.org/going-digital/trade-in-the-digital-era.pdf).

Papaconstantinou, G A (2020), "The GATS and financial regulation: Time to clear-house?", *World Trade Review* 19: 379–401.

Peihani, M (2015), "The Basel Committee on Banking Supervision: A post-crisis assessment of governance and accountability", *Canadian Foreign Policy Journal* 21(2): 146-163.

Rentzhog, M (2015), "No transfer, no production — A report on cross-border data transfers, global value chains, and the production of goods", *Kommerskollegium* 2015:1, National Board of Trade Sweden.

Rentzhog, M and H Jonströmer (2014), "No transfer, no trade — The importance of cross-border data transfers for companies based in Sweden", *Kommerskollegium* 2014:1, National Board of Trade Sweden.

Riepe, J (2019), "Basel and the IASB: Accountability interdependencies and consequences for prudential regulation", *Journal of International Economic Law* 22: 261–283.

Roger, C B (2020), *The origins of informality: Why the legal foundations of global governance are shifting, and why it matters*, Oxford University Press.

Ruder, D S, C T Canfield and H T Hollister (2005), "Creation of worldwide accounting standards: convergence and independence", *Northwestern Journal of International Law and Business* 25(3): 513–88.

Schoenmaker, D (2013), Governance of international banking: The financial trilemma, Oxford University Press.

Tweedie, D and T R Seidenstein (2005), "Setting a global standard: the case for accounting convergence", *Northwestern Journal of International Law and Business* 25(3): 589–608.

Viterbo, A (2019), "The European Union in the transnational financial regulatory arena: The case of the Basel Committee on Banking Supervision", *Journal of International Economic Law* 22: 205–228.

WTO (2018), *The future of world trade: How digital technologies are transforming global commerce*, World Trade Report 2018.

Yokoi-Arai, M (2008), "GATS' prudential carve out in financial services and its relation with prudential regulation", *The International and Comparative Law Quarterly* 57(3): 613-648.

Yoo, J Y and D Ahn (2016), "Security exceptions in the WTO system: Bridge or bottle-neck for trade and security?", *Journal of International Economic Law* 19: 417-444.

ABOUT THE AUTHOR

Patrick Leblond holds the CN-Paul M. Tellier Chair on Business and Public Policy and is an Associate Professor in the Graduate School of Public and International Affairs at the University of Ottawa. He is also Senior Fellow at the Centre for International Governance Innovation (CIGI), Research Associate at CIRANO and Affiliated Professor of International Business at HEC Montréal. Dr Leblond is an expert on economic governance and policy with a particular focus on Canada, North America, Europe and, increasingly, China. He has published extensively on financial and monetary integration, banking regulation, international trade, data governance, and business-government relations.

CHAPTER 7

Rights in data, the public interest, and international trade law

Teresa Scassa[1]
University of Ottawa

INTRODUCTION

The global economy is increasingly dependent on data as fuel for high-tech industries. Chief among these is the data-thirsty artificial intelligence (AI) industry, which is the focus of intense global competition. Furman and Seaman (2019) have documented how, across a broad range of metrics, AI-related innovation and investments are growing rapidly. Countries are struggling to position themselves in the race to dominate in this field (Westerheide 2019). Data is the fuel of AI innovation, and the importance of data can be seen in measures such as the EU's recast "Directive on open data and the re-use of public sector information".[2]

Data is acquired or generated by various means. It can be gathered by environmental or other sensors, acquired through the course of business operations, or generated through research. Personal data, which carries enormous commercial value, is harvested from the digital activities of individuals; derived data is also created through analytics, profiling and other forms of processing. Governments hold important stores of data that result from the carrying out of their functions, including their regulatory functions, as well as their interactions with residents. Non-personal government data is increasingly released as open government data under policies designed to support data-driven innovation (Kitchin 2014, Directive (EU) 2019/1024).

Just as data is at the heart of much innovation and competition, issues relating to access to and use of this data are linked to a broad range of public interests. These can include transparency and accountability, privacy, public health and safety, national security, and economic growth and development. These interests are sometimes in conflict with one another – for example, transparency and accountability may require providing access to data; data protection laws may limit access to some kinds of data; and economic development may require increased access to data for some, as well as some degree of

1 My thanks to Matt Malone for his research assistance. Many thanks as well to Ingo Borchert and L. Alan Winters for their thoughtful feedback on an earlier draft.

2 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019 (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024).

exclusivity and control over data. The data-driven nature of the AI industry has brought the competing public interests in access to and use of data sharply into focus. As Mishra (2020) notes, the enormous economic and social benefits promised by AI are countered by significant risks of harm, including exploitation, discrimination, and manipulation. Data is needed both to fuel AI and to hold it accountable. Governments are still articulating national data strategies, and there is considerable ongoing work around ethical AI governance. Public policy debates pertain to open data, data localisation, data sovereignty, data protection, data security, and data transparency. As Aaronson and Struett (2020: 8) note, "[n]o one really knows yet what good governance of data looks like."

At the same time as countries struggle with domestic data policies, the international community continues to develop and expand digital trade rules. The economic importance of data means that the free flow of data across borders is a trade priority. Thus, attention is paid to those things that might present barriers to data flows, such as data protection and data localisation requirements. Provisions addressing these issues are becoming commonplace in the digital trade sections of international trade treaties.

While recognising the importance of the tension between the free flow of data and data protection concerns, this chapter considers a different set of issues with trade and data policy. It confronts the challenge that lies at the intersection between the protection of data as intellectual property (IP) – whether copyright, trade secret, or both – and the expanding public interest in access to such data in a broadening range of contexts. The issues here are claims to property interests in data on the one hand, and claims to rights to access, rely upon and/or use such data in the public interest. The chapter suggests that these tensions are already reflected in international trade agreements to some extent, but that the rapid growth of digital and data economies may require new attention in order to accommodate the growing importance of data and complex and evolving public interests. It considers how these competing interests are navigated by international trade agreements, the tension between AI data governance, and the protection of trade secrets and confidential information.

This chapter considers the scope of protection of data as IP, with a focus on copyright law and the law of confidential information; the extent to which the public interest in data is reflected in exceptions/limitations to protection of intellectual property rights (IPRs) in data; the relationship of IPRs in data to data protection law; and data and the public interest. For the sake of scope, the chapter focuses on provisions in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)[3] and the recently negotiated Canada–United States–Mexico Agreement (CUSMA).[4] The chapter begins with a brief account of an investor–state dispute over data brought against Canada under

3 Agreement on Trade-Related Aspects of Intellectual Property Rights, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994).

4 Note that the title of the Agreement varies by nation; I am using the Canadian version.

the North American Free Trade Agreement (NAFTA), which is yet to be resolved. This case highlights some of the issues in the clash between data as IP and the public interest in data.

THE *GEOPHYSICAL* DISPUTE

In 2018, three US investors filed a claim to arbitration under Chapter 11 of NAFTA on behalf of Geophysical Service Incorporated (GSI) (henceforth, "Einarsson Claim, 2018").[5] The claim followed a series of lawsuits in Canada brought by GSI against the Canadian government and its agencies, as well as private sector corporations regarding IP rights in GSI's data. The lawsuits involved 41 defendants in a total of 25 court actions. GSI was ultimately unsuccessful in this litigation.

Between 1969 and 2009, GSI and its predecessors were engaged in the creation of compilations of marine seismic data from Canada's offshore waters. The collection and processing of this data was a complex endeavour requiring specialised equipment and highly skilled personnel. Once the process was completed, GSI licensed its proprietary data to oil and gas prospecting companies under contracts that asserted copyright in the compilations and provided that the information also be kept confidential. In order to carry out its seismic surveying in Canadian waters, GSI required regulatory permission, which it obtained. As a condition of the grant of permission to conduct its seismic surveying in Canadian waters, GSI was required to submit information about its activities along with a copy of its seismic data to Canada's National Energy Board (NEB), and to the Canada Newfoundland and Labrador Offshore Petroleum Board and the Canada Nova Scotia Offshore Petroleum Board (henceforth, 'the Boards'). GSI maintains in its NAFTA claim that although the requirement to submit data was in place since the beginning of its activities, the initial practice was that the data were kept confidential. They claim that the government's practice changed over time "as policy and technology evolved".[6] It should be noted that the format of the submitted data changed over time (from paper copies to digital data), opening up new possibilities for reuse. As data analytics and AI evolved, it is not difficult to see how the scope and scale of reuse of data might also expand.

Between 2000 and 2010, GSI learned through a protracted series of access to information requests that its confidential data was being shared, without notice, with many of the companies with which GSI previously had licensing agreements. In effect, it learned that after the expiration of a confidentiality period, the data submitted to the Boards was made public. At the heart of the dispute is what happened to the data once submitted to

5 Theodore David Einarsson, Harold Paul Einarsson and Russell John Einarsson, Geophysical Service Inc. and Government of Canada, Notice of Intent to Submit a Claim to Arbitration under NAFTA Chapter 11, October 10, 2018 (www.geophysicalservice.com/Uploads/NAFTA_Claim.pdf). Einarsson Claim, 2018. Under CUSMA, the investor–state dispute resolution mechanisms are found in Chapter 14. However, these will only apply to disputes between the US and Mexico, as Canada has opted out. Legacy claims such as the Geophysical Claim will continue in accordance with Chapter 11 of NAFTA.

6 Einarsson Claim, 2018, at para. 8.

the government agencies. GSI maintained that the data was always intended to remain proprietary and confidential. The government took the position that regulatory approval was required to conduct the seismic surveys, and that the subsequent use of the data, "including the deposit of the material, the term of confidentiality and public access to it, is strictly regulated by legislation ('the Regulatory Regime')". According to the government, "[t]he Regulatory Regime vests only certain rights and allows the copying of the material in question after the confidentiality period has expired".[7]

On learning of the data sharing, GSI sued the Canadian government for breaching its rights; it also brought suit against the private sector companies that used the data published by Canadian authorities without license from GSI. In 2016, the Alberta Court of Queen's Bench decided that GSI had valid copyrights in its compilations of seismic data. However, it also ruled that the regulatory regime established by the government effectively cut short the term of copyright protection.[8] Essentially, the regulatory regime was interpreted as taking precedence over the copyright protection; a surrender of copyright after a prescribed confidentiality period was the statutory quid pro quo for a licence to conduct the seismic testing. The decision was upheld on appeal to the Alberta Court of Appeal[9] and leave to appeal to the Supreme Court of Canada was denied.[10]

In its NAFTA arbitration claim, GSI argues that Canada breached its obligations under the Investment chapter of the agreement. GSI's claims are based upon its asserted IPRs in the data, grounded on copyright and trade secret protection.[11] In terms of the confidential and proprietary information at issue, GSI argues that Canada breached the Article 1106 guarantee that an investor will not be required "to transfer technology, a production process or other proprietary knowledge to a person in its territory". It also argues under Article 1110 that the regulatory regime amounted to an improper expropriation, without compensation, of its proprietary and confidential information. When this dispute is heard, it will assess the legitimacy of the Canadian regulatory scheme that required data to be submitted to the regulator in exchange for permission to operate and that brought an early end to copyright protection. In domestic litigation, the government stated that the regulatory scheme "balances two competing policy objectives: the objective of protecting confidential information long enough to allow for recuperation of the expenses incurred in undertaking a non-exclusive seismic project *against the objective of stimulating natural resource exploration and development by making such information publicly available*"[12] (emphasis added).

Although this example is specific to its own facts, and different from situations that might arise in other contexts, including in relation to AI regulation, it illustrates the potential conflict between the protection of proprietary data and state interests not just in accessing

7 *Geophysical Service Incorporated v Encana Corporation*, 2016 ABQB 230 (CanLII), at para. 6 (https://canlii.ca/t/gppg3).
8 *Geophysical Service Incorporated v Encana Corporation*, 2016.
9 *Geophysical Service Incorporated v EnCana Corporation*, 2017 ABCA 125 (CanLII) (https://canlii.ca/t/h3jnp)
10 *Geophysical Service Incorporated v. EnCana Corporation, et al.*, 2017 CanLII 80435 (SCC) (https://canlii.ca/t/hp1c1)
11 Einarsson Claim, 2018.
12 *Geophysical*, 2016, at para. 123.

that data, but in determining the uses to which it might be put. It raises a complex issue of 'interests' in data. We are most used to seeing this in the context of personal data, where companies may collect and compile personal data but individuals retain an interest by way of data protection law. Arguably, in this case, a government claims a national interest in data from its offshore waters – an interest that is protected through disclosure requirements in a regulatory regime that controls access to those waters for seismic exploration. The alleged breach in this case highlights the tension between the public interest asserted by the government and the private rights of the owner of IPRs.

PROTECTING DATA AS INTELLECTUAL PROPERTY

There is no distinct IP regime for the protection of data. This section considers the two main areas of IP law that can be used to protect data or compilations of data in some circumstances: copyright law and the law of trade secrets/confidential information.

Copyright law

TRIPS reflects an international baseline consensus regarding the protection of IP in the context of international trade. It recognises the protection of data broadly under IP in two main areas. The first of these is copyright. With respect to copyright and data, Article 10(2) of TRIPS provides:

> 10(2). Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.

This provision recognises that compilations of data can be protected in copyright law so long as they reflect an original selection or arrangement. Such protection is limited since the expression protected by copyright lies in how the data is selected or arranged. However, Article 10(2) leaves open the possibility that there may be separate protection in "the data or material itself". Recognising a separate protection for the material in a compilation is relatively easy if one thinks of a compilation of copyright protected works (e.g. an anthology). There can be a copyright in the compilation as well as separate copyrights in the individual works included in the compilation. It is more challenging to see a separate copyright in data included in a compilation. Facts have long been considered to be part of the public domain (dusollier 2010). Facts are the building blocks of knowledge, and the goal of copyright law is to protect original expressions of knowledge rather than to allow facts or ideas to be monopolised. Although copyright recognises the potential for originality in a compilation of facts, the originality lies in the selection or arrangement of those facts, rather than in the facts themselves (Shipley 2007, Bitton 2009). The fragility of copyright protection for compilations of facts was made evident in the watershed US

Supreme Court decision in *Feist Publications, Inc. v. Rural Telephone Service, Co.*[13] This decision disrupted conventional industry expectations that the investment of labour or money in the creation of compilations of facts was enough to ground their protection under copyright law. In *Feist*, the court found that the banal selection and arrangement of telephone directory data meant that there was no originality in a compilation of such data. The case sent shockwaves across the Atlantic, leading eventually to the adoption of the 1996 Database Directive[14] in the EU. Yet even the *sui generis* database right created in that Directive has not proved well-adapted to the contemporary data economy, as it focuses on the efforts expended to create a database rather than on the efforts expended to create data itself (Hoeren 2014). In this sense, it is inadequate to protect data that is generated in the normal course of business, as opposed to being collected and compiled for a specific purpose (Banterle 2016). The result has been unsatisfactory and uncertain protection for data in copyright law. There is a tension here – the protection of assets serves established industries, but less protection for data may help fuel innovation, particularly in an expanding data economy.

More recently, some courts in copyright cases have started to draw a distinction between 'data' and 'facts', with facts being in the public domain and data reflecting some form of processing that can be close to authorial effort (Scassa 2018). Nevertheless, this distinction is still not one that can reliably lead to copyright protection. In the US, for example, even courts that have found a degree of authorship in data have applied the merger doctrine to find that copyright protection is not available (Scassa 2018). The merger doctrine provides that where facts (or ideas) cannot be separated from their expression, then they cannot be protected by copyright law since to provide protection is to give a monopoly over the underlying fact or idea.

In spite of the limits of copyright law in this area, copyright remains an avenue for the protection of compilations of data. The emerging tendency in some courts to distinguish between data and facts, as discussed above, may mean that the protection available for compilations of data may be more robust than for compilations of fact. While data individually may not be capable of copyright protection even if it is 'derived' and not 'observed', compilations of derived data may well be considered inherently to reflect a high degree of originality in selection or arrangement that make them easier to protect. Indeed, the court's reasoning in *Geophysical* (2016) suggests that the seismic data collected by the company would have a degree of inherent originality that would make them easy to protect. Copyright law is thus still a viable option for protecting compilations of data. Challenging questions will arise, however, as to the originality of some compilations of data, especially if machine generated. There may also be issues as to the originality of data formatted for submission as part of government regulatory processes. Data may be easier to protect than facts, but there will still be significant challenges in some cases.

13 *Feist Publications, Inc., v. Rural Telephone Service Co.*, 499 U.S. 340 (1991).
14 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009).

The lack of reliable protection for data and compilations of data has led to discussions (chiefly in Europe) about the need for a *sui generis* data ownership right (Drexl et al. 2016, Farkas 2017, Hugenholz 2017). These discussions have struggled with many challenges, including the diverse interests that may exist in data, the difficulty of assigning ownership to data, and the problems of balancing ownership rights with complex competing interests, including the public interest (Drexl et al. 2016, Centre for Information Technology, Society and Law 2017). To date, a separate ownership right for data has failed to gain traction.

The result is that currently international trade agreements such as CUSMA provide the scope to protect data under copyright law and the latitude for developments in this area, but do not address it in any new ways. Debates in the EU over data ownership rights highlight the nascent state of such discussions and reveal the major challenges in creating any new frameworks for protecting 'ownership' rights in data.

Trade secrets/confidential information

The other main way to protect data in IP law is as a trade secret or confidential information. The two terms describe different manifestations of the same concept. 'Confidential information' is typically used to refer to confidential business information (for example, customer data or business plans), while 'trade secrets' refers to knowledge with an industrial application (for example, algorithms, industrial 'know-how', formulae) (Hagen et al. 2018).

Trade secret rights are challenging to fit within conventional property frameworks. Data is typically non-exclusive and non-rivalrous, as it can be possessed and used by many at the same time. In addition, there may be multiple interests in data – especially with personal data. The ability of owners of trade secrets to protect them in the digital and data economy is impacted by the ease of copying and transmission.

TRIPS requires states to protect "undisclosed information" in certain circumstances. According to Article 39(2) of TRIPS, information is eligible for such protection if it:

> (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> (b) has commercial value because it is secret; and
>
> (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

The same principles apply to both confidential information and trade secrets. When it comes to data, trade secret law protects not the data per se, but rather efforts made to protect its confidentiality. Even if a database contains publicly available data, the database as a whole may still be capable of protection as a trade secret if the compilation

of that data in one place makes it unique and valuable if kept confidential. Trade secrets are protected only so long as they remain secret, making such protection inappropriate for some categories of data, depending on how it is meant to be used or exploited. For example, data that is published or that is made available through a searchable database is not confidential, and other forms of protection (database protection, copyright, contract law, etc.) are required. Trade secret rights can be lost if data is insufficiently protected and/or publicly shared. While it is sometimes possible to use legal interventions to protect trade secrets after a breach (for example, using injunctions to prevent a wrongdoer from further sharing the confidential information), there is also the risk that protection can be lost. As a result, the duration of protection for trade secrets can range from theoretically perpetual to transient, depending at least in part on the efforts made by the 'owner'.

The trend in so-called 'TRIPS-plus' agreements has been towards the enhancement of protection for IPRs, including trade secrets. To a large extent, these extended protections recognise the importance of IP assets in an expanding digital and data economy.

CUSMA, for example, builds upon the TRIPS provisions. While the basic definition of trade secrets in CUSMA remains the same as that in TRIPS (see Art 20.72), CUSMA is more specific as to the meaning of 'misappropriation' in the context of trade secrets, defining not just what activities constitute misappropriation, but also which ones (e.g. reverse engineering, independent discovery, or legitimate acquisition) do not (Art. 20.72). The CUSMA obligation to protect trade secrets is also enhanced over TRIPS:

> **Article 20.69: Protection of Trade Secrets**
>
> In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention, each Party shall ensure that persons have the legal means to prevent trade secrets lawfully in their control from being disclosed to, acquired by, or used by others (including state-owned enterprises) without their consent in a manner contrary to honest commercial practices.

The obligation shifts from the TRIPS requirement to give persons "the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent", to the firmer "ensure that persons have the legal means to prevent trade secrets lawfully in their control from being disclosed to, acquired by or used by others" without consent (Art. 39(2)).

The enhanced protection of trade secrets in international trade treaties is linked to the growth of industrial espionage in high technology industries. In 2011, trade secret theft was identified in the US as a growing threat to national prosperity and security (Office of the National Counterintelligence Executive 2011). The Congressional Research Service (2020: 23) noted the American preoccupation that "China may likely gain access to U.S.

commercial development in AI given its extensive history of industrial espionage and cyber theft". These concerns were a motivation, for example, to require stronger trade secret protection in CUSMA.

To supplement this stronger wording, CUSMA contains additional provisions setting requirements for both civil protection and enforcement and criminal enforcement of trade secret rights (Arts. 20.70 and 20.71). States party to the agreement may not limit the duration of protection for trade secrets so long as the conditions for subsistence of a trade secret exist (Art. 20.70(b)). Articles 20.73 and 20.74 specifically address confidentiality of trade secrets in judicial proceedings to enforce trade secret rights. Notably, however, this does not address the protection of trade secrets or confidential information that may arise in the context of other types of litigation (for example, civil litigation relating to AI). Article 20.75 requires a minimum level of civil remedies available in the case of breaches of trade secret rights (damages and injunctive relief).

Just as copyright law has limits in protecting data, so too does trade secret law. In the common law legal tradition, trade secrets are protected largely by the law of equity and the common law, and thus have historically been a non-statutory body of law (OECD 2015, Hagen et al. 2018). In the EU, trade secret protection similarly draws on a diffuse range of legal regimes, from contract to unfair competition law (Banterle 2016). The peculiarities of trade secret law may also mean that in federal states, trade secret protection is not national, but rather occurs at the regional (state/provincial) level. This trend may be starting to shift; for example, the US government recently passed the Defend Trade Secrets Act of 2016 at the federal level.[15] This statute creates a private right of action at the national level.[16] It is no accident that this step has come with the growing importance of trade secrets to the burgeoning digital and data economy in that country.

The fact that trade secret law is non-statutory in some jurisdictions (and that it is left to state/provincial governments in federal states) can make it difficult in international law both to identify commonalities and to be as prescriptive, as is the case with other areas of IP law. For example, the copyright, trademark, and patent law provisions of TRIPS and the domestic laws as well as international treaties that have followed TRIPS (collectively, 'TRIPS-plus') are all founded on international IP conventions that have long shaped domestic statutory regimes, such as the Berne Convention (1886)[17] and the Paris Convention (1883).[18]

From a public interest perspective, trade secret law also presents unique challenges compared to other areas of IP law. While statutory areas of IP protection such as patent and copyright law balance private rights with the public interest through term limitations,

15 *Defend Trade Secrets Act of 2016*, PL 114-153, 130 Stat 376 (2016).
16 *Defend Trade Secrets Act*, s. 2(b).
17 *Berne Convention for the Protection of Literary and Artistic Works*, September 9, 1886, as revised at Stockholm on July 14, 1967, 828 U.N.T.S. 221.
18 *Paris Convention for the Protection of Industrial Property*, as last revised at the Stockholm Revision Conference, Mar. 20, 1883, 21 UST 1583; 828 UNTS 305.

exceptions, and other measures found in the same legislation that establishes the rights, there is generally no unified regime for trade secrets and their exceptions. Legally, trade secret protection can last as long as confidentiality is maintained. In practical terms, rights holders can implement a variety of measures to preserve confidentiality. Although exceptions to trade secret protection may exist, these are found scattered across legislation that addresses different public interests in different contexts. This feature of trade secret law suggests that the management of these exceptions might appear separately in international trade treaties as well.

Emerging policies for ethical AI will need to address the need for oversight and accountability of algorithms and training data, both of which may be protected as trade secrets (Floridi et al. 2018, European Commission 2020, Schmelzer 2020). Balancing public and private interests in these contexts may be complex and multifaceted. Some data protection laws already contain provisions regarding the right to an explanation of automated decision making, although it is not always clear what level of transparency will be required by such provisions (Edwards and Veale 2017, Casey et al. 2019). Data protection laws also typically contain a right of access to one's personal data. This right of access may create tension between the personal data rights of the individual and the rights of organisations. For example, concerns have been raised that too much transparency with respect to data and/or algorithms can lead to the gaming of algorithms, or their reverse engineering (Yakowitz Bambauer and Zarsky 2018).

As the digital and data economy expands, the public interest in data will manifest itself in new ways. Just as seismic data can drive oil and gas prospecting, other data may have economic implications for countries. Many countries hold data that has a high commercial value and are contemplating the potential to derive value from this data in terms of revenue, innovation or other benefits (e.g. MacGregor 2018). Countries with publicly funded health care systems, for example, sit on valuable troves of health data (Aggarwal 2018). Israel has recently traded access to personal health information in exchange for COVID-19 vaccinations (Lovell 2021, Ravia et al. 2021). Other governments have also contemplated ways to exploit their stores of health data (Dickens 2020).

While there is nothing yet in trade agreements that addresses these developments, it is important to note first that this is a rapidly changing and evolving landscape; that many nations have yet to determine how to manage their stores of data in the public interest; and that doing so might mean setting rules limiting access to this data or imposing conditions on its use. In some cases, it might also require private sector partners – or private sector participants in particular sectors – to contribute data as a condition of participation in the sector (as was the case in *Geophysical*). How such measures fit within international trade law frameworks will be an important issue.

It is in such contexts where laws provide for the disclosure of trade secrets or confidential information in the public interest, that the differences between trade secret law and other areas of IP law become more noticeable. The balancing of interests which takes

place in copyright and patent laws, for example, addresses the specific interests of known categories of users, measured against the interests of rightsholders. This is done through subject-matter limitations, fair use, and other exceptions. It is also done by limited terms of protection. Trade secret protection is potentially perpetual, although the broad range of contexts where it can be limited by government in the public interest suggests that it is a much more modulated form of protection. Nevertheless, the public interests are diffuse and varied, and they are addressed across a broad range of legislative and regulatory regimes.

DATA AND THE PUBLIC INTEREST IN INTERNATIONAL TRADE LAW

Issues around data and the public interest in international trade law will inevitably take on more importance as data itself assumes a greater role as fuel for the digital and data economy. In the previous section we considered IPRs in data. In this section, we consider public interest exceptions to these rights.

There is nothing in TRIPS that specifically prevents states from "demanding access to technical information when it is necessary to protect public interests" (Mishra 2020: 43). Further, as Mishra notes, Article 8(1) of TRIPS allows states to implement measures to protect the public interest. However, Mishra also notes that TRIPS-plus treaties may be encroaching on this latitude by enhancing IP protection and through limits to exceptions. An important subset of exceptions to IPRs in confidential information is found in diverse regulatory systems and government policies that require either the sharing of confidential information with government agencies or regulators, or its public disclosure – or both.

TRIPS addresses requirements to submit confidential information as part of regulatory regimes. Article 39(3) requires that regulatory approval data shall be protected "against unfair commercial use" (Gleeson et al. 2019, Yu 2018). Yu describes this provision as reflecting "the different compromises between developed and developing countries during the TRIPS negotiations" (p. 3) As is the case with other TRIPS-plus treaties, CUSMA (like NAFTA before it) contains additional protection for data exclusivity in these contexts. The new CUSMA provisions are found in the patents section, rather than the trade secrets section. This is because the regulatory regimes at issue are for the approval of pharmaceutical and agricultural chemical products, and are linked to the term of patent protection. Regulatory regimes that permit reliance on safety data submitted by the patent-holder in the regulatory approval process give an advantage to the generic manufacturers. At the same time, they serve the public interest by allowing faster entry onto the market of the generic product, thereby increasing access to medicines and lowering costs (Yu 2018). As the US Supreme Court noted with respect to a similar

regulatory regime for agricultural chemical data, the public interest lies in "eliminat[ing] costly duplication of research and streamlin[ing] the registration process, making new end-use products available to consumers more quickly".[19]

Although CUSMA contains data exclusivity provisions related to both agricultural chemical products and pharmaceutical products, the obligations are more stringent for pharmaceutical products, reflecting the dynamics of different regulatory and economic contexts. Data exclusivity requirements do not prevent countries outright from enabling data access in a regulatory regime. However, they do limit it and impose conditions designed to ensure that innovator companies are not deprived of the full commercial advantage of the confidentiality of such data (Thrasher et al. 2019). Thus, for example, Article 20.45 provides that the confidentiality of data concerning the safety and efficacy of agricultural chemical products must be preserved for "at least 10 years from the data of marketing approval of the new agricultural chemical product in the territory of the Party". In the case of pharmaceutical products, Article 20.48 provides for the confidentiality of data concerning the safety and efficacy of the product "for at least five years from the date of marketing approval of the new pharmaceutical product in the territory of the Party". Article 20.48(1)(a) of CUSMA specifically requires states to compensate for any reliance permitted on confidential data submitted for regulatory approval processes by placing time restrictions on the market entry of any generic product, the approval of which is based on the confidential data. The provision also establishes a set of qualifications to this exception based upon public health exigencies. Similar provisions were found in NAFTA, but there is considerably more detail in CUSMA and the protection of private interests is more robust. Thrasher et al. (2019: 13) note that the enhanced enforcement provisions in TRIPS-plus treaties "give additional teeth" to these measures. Gleeson et al. (2019: 2) are critical of these provisions, because of their impact on other public interests. They note that data exclusivity requirements are among those "now commonly included in trade agreements [that] can impinge on access to safe, effective, quality and affordable medicines, potentially undermining the achievement of universal health coverage and the SDGs".

Although current data exclusivity provisions have been linked to patents and are specific to particular industries, they are important to consider in the emerging context of AI regulation. Currently many countries are considering how best to regulate AI for the purposes of safety, security, as well as ethics and human rights. In such contexts, some governments may actually require the disclosure of data and/or algorithms as a condition of providing AI to government; as part of algorithmic oversight systems; or in relation to algorithmic accountability processes. Where this takes place, there will no doubt be consideration given to how such disclosures must be made, to whom, and under what conditions (insofar as they are designed to protect IP interests). The data exclusivity provisions for pharmaceutical and agricultural product data illustrate how international

19 *Ruckelshaus v. Monsanto*, 1983, p. 986.

trade treaties can set parameters for competing private and public interests. In the case of pharmaceuticals, for example, the established nature of the regulatory regimes that predated the trade treaty provisions likely strengthened the hands of those states that have permitted reliance on regulatory data. In the AI context, there is a risk that new digital trade provisions in international trade might strongly protect private interests in the confidentiality of data before the public interest in access to this data has had a chance to be framed and articulated in legislation or in regulatory regimes.

The *Geophysical* case is an instance where the sharing of data after a limited confidentiality period was the legislated quid pro quo for a licence to collect the data. Article 20.70(b) of the CUSMA provides that states may not limit the duration of the protection of trade secrets so long as the conditions for subsistence of a trade secret exist. If such a regulatory approach is seen to limit the duration of trade secret protection, then it would run afoul of such a provision. Serious consideration should therefore be given to the implications of provisions of this kind for regulatory mechanisms that make data sharing a condition for access to the space or resources necessary to generate the data.

DATA-RELATED LAW AND POLICY WITH IMPLICATIONS FOR IPRS IN DATA

Data protection

The above discussions relate to the challenges of protecting commercially valuable data. One of the most valuable categories of data in the digital and data economy is personal data. Data protection laws negotiate the rights of individuals vis à vis those who seek to harvest and use their data. Data protection laws limit how organisations can collect, use, or disseminate data. They also limit the retention of personal data. Data protection laws can place limits on an organisation's rights in their confidential commercial data where that data is also personal data. In addition to the more conventional data protection limits and controls such as consent and purpose limitation, the EU's 2018 General Data Protection Regulation (GDPR) has introduced new individual rights of control over personal data. These include a right of erasure that enables individuals to withdraw data from processing activities (Article 17). The GDPR's data portability right in Article 20 enables individuals to demand a machine-readable copy of their data in the hands of an organisation for the purposes of 'porting' it to another organisation. The right to an explanation in the automated decision-making context might also have some impact on the ability of organizations to maintain secrecy regarding the data they use in such processes. The GDPR – along with its predecessor, the Data Protection Directive (1995)[20] – has had considerable global influence because it expressly limits the flow of personal data of EU residents to only those countries or contexts in which a level of data protection deemed adequate is available. The recent decision in *Data Protection Commissioner v.*

20 *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 24 October 1995 (www.refworld.org/docid/3ddcc1c74.html).

Facebook Ireland Ltd., Maximillian Schrems (2020),[21] demonstrates how inadequate data protection laws can pose a significant barrier to the free flow of data (Patel and Lea 2020).

In addition to basic data protection laws, some national governments have also adopted data localisation requirements for specific categories of data, which can also impact the free flow of data (Chander and Le 2015). Although data localisation laws may specifically address data protection concerns, some data localisation measures seek to ensure that states maintain access to data for law enforcement or national security purposes (Hill 2014, Chander and Le 2015). Some may also be linked to economic protectionism (Hill 2014) as well as to sovereignty concerns (De Filippi and McCarthy 2012). These mixed objectives make them harder to address in trade agreements as, for example, protectionism could be couched as privacy concerns. Data localisation and data sovereignty measures are, of course, more important for those countries that are not home to large data giants, platform companies, or providers of cloud services. Although beyond the scope of this chapter, it is worth noting that limits on data localisation are already being negotiated into TRIPS-plus agreements, including CUSMA (see CUSMA, Art. 19.11). New models of data governance in contexts that involve personal data, or data derived from communities such as smart cities, have also led to growing data nationalism as well as to calls for data localisation measures based on a mixture of concerns over domestic innovation agendas, sustainability, and privacy (Scassa 2020). These considerations can impact the public interest dimensions of confidential information that is also personal data.

It should be noted as well that some scholars have argued for individual ownership rights in personal data (Baron 2012, Ritter and Mayer 2016, Trakman et al. 2019), in ways that enhance control, even allowing them to participate in the brokerage of these data (Haupt 2016, Dennedy and Liezeroy 2017). Although these views are not necessarily consistent with data protection regimes such as those in the GDPR, they have gained traction in some quarters. Some proposals are relatively simple, others more complex and detailed. For example, Snower and Twomey (2020) have proposed a 'digital barter' system for personal data governance by enhancing individual rights of control over personal data, effectively altering the economic structure of data markets (Snower et al. 2020). Arguments in favour of these new concepts of personal data ownership presume a certain latitude among national governments to enable such a shift in the nature and location of data 'ownership' rights – something that might impact on existing IP rights in data.

Data sharing and data mobility

Frameworks for the sharing of data and for data mobility are a matter of active policy development. For example, in the context of pharmaceutical products, Yu (2018) notes the development of data sharing frameworks for clinical trial data by the Euromedicines

21 Case C-3118, 2020.

Agency (2014), as well as data sharing recommendations of the UN Secretary-General's High-Level Panel on Access to Medicines (2016). Data portability under the GDPR gives individuals the right to move their data from one provider to another. Some have linked this right to consumer protection and competition law goals more than to the protection of privacy (Graef et al. 2013). Portability requirements have raised the issue of whether there needs to be a distinction between data obtained from the individual directly and derived data. The distinction between the two could recognise the greater proprietary interest that organisations might have in data that has been derived from personal data through analytics or other processing. In open banking, already under way in some jurisdictions, including the UK and the EU (Borgogno and Colangelo 2020, Morvan 2020), the state creates a framework for interoperable data within a commercial sector to facilitate data mobility, enhancing competition within that sector. The other name for open banking – consumer-directed finance – plays up the element of individual control over personal financial data within that sector. Such frameworks offer significant potential both for innovation and for the protection of consumer and data privacy interests. Yet they are also – of necessity – heavily regulated and may raise issues regarding the free flow of data. A core part of open banking – or any other structured sectoral data mobility frameworks – is the governance of data, including data standardisation, data security rights, and data portability rights for individuals.

The rethinking of control over personal data in certain sectors, and the incorporation of new paradigms into regulatory frameworks, has the potential to disrupt conventional notions of data ownership and control of commercial data. For example, in the evolving connected and automated vehicle context, there is emerging debate in Europe, at least, over how access to and use of connected vehicle data will be controlled. Early claims of 'ownership' rights in the original equipment manufacturer (OEM) have met with competing visions in which individuals determine who is to have access to vehicular data and on what conditions (Kerber 2018). Frameworks for the brokering of data access and use on behalf of individuals have gained traction in the EU, bolstered by a strong data protection infrastructure (Snower and Twomey 2020).

These new modes of governing data – particularly personal data – seek to balance individual and community rights against commercial rights in data. They do so in the public interest – but also within a context in which both the technology and the means of structuring its governance are rapidly evolving. They call for a kind of flexibility that can facilitate innovation – not just in digital technologies but in their governance.

Artificial intelligence governance

Countries are exploring data strategies to ensure their competitiveness and their ability to innovate, along with their access to crucial data in the evolving data economy. As Aaronson and Struett (2020: 8) note, "[b]ecause data is so important, many nations are

adopting national strategies, such as AI plans, data strategies or data charters, to nurture the data-driven economy [. . .]. However, some of these national plans and strategies may make it harder for data to flow across borders."

The potential for data to drive automation in everyday devices and in decision making across public and private sectors creates contexts in which the public interest in access to data is important, if not essential, to address health or safety concerns, assess accuracy and quality of output, and monitor for and address discrimination and bias (Citron and Pasquale 2014, Floridi et al. 2018). This prompts demand for access to data in a variety of contexts. This can include personal injury litigation on small or large scales (for example, in relation to autonomous vehicles, including aircraft, or medical malpractice relating to algorithm-driven diagnosis or treatment) (Lim 2018). Challenges to automated decision-making processes can also lead to demands for the disclosure of data or algorithms. Such decisions could be specific to particular individuals in private sector contexts (for example, challenging a denial of credit, accommodation, or insurance), or they could drive class-action litigation in relation to similar issues affecting large numbers of people. Challenges to algorithms used in the public sector could include those used in the criminal or carceral context, or those used for public sector automated decision making more generally. This is an area of public policy that is growing in importance and still very much in the process of development. Rules that develop around access to data and algorithms in the litigation context would need to protect confidential information while allowing adequate access to data.

Growing demands for ethical and responsible AI development and adoption have led some governments to push for the implementation of automated-decision-making systems that include the scope to review or assess algorithms for things such as fairness, bias, and discrimination (e.g. AI HLEG 2019, European Commission 2020). The ability to review data and/or algorithms may also be important for governments that want to ensure the safety of critical systems. Data protection laws, recognising the interests of individuals in their personal data, also increasingly provide for some level of algorithmic and data transparency through rights to an explanation where personal data is used in algorithmic decision-making processes (Edwards and Veale 2017, Casey et al. 2019). Again, this is an area of public policy that is in the process of development. It is also a technological domain that is in rapid evolution. While on the one hand there is a potential impact on trade secret owners, on the other hand, the public interest can shape the evolution of technological solutions. Limitations on policy options in trade agreements may not just limit the development of public policy (Mishra 2020), they may also limit the ability of the public interest to shape the features of technological development. Mishra (2020) suggests a need for specific provisions in international trade treaties to address the protection of human rights, ethical design, and algorithmic accountability – creating specific room for the development of such approaches. She notes that "[h]ighly restrictive Data Ethics-related Measures may violate obligations contained in international trade agreements.

Therefore, the issue arises as to whether international trade agreements restrict the ability of governments to protect or promote data ethics-related policy objectives" (Mishra 2020: 5).

CONCLUSION

This chapter has considered how IPRs in data – notably copyright and trade secret law – can impact on a broad range of data governance issues. Since TRIPS in 1994, international trade agreements have made IP obligations a common feature, and the protection of IP rights continues to expand through these vehicles. The expansion of IP obligations in TRIPS-plus treaties could therefore impact on data governance in complex ways. In the case of data, the two most relevant IP categories are copyright and trade secrets.

A particular challenge will be the balancing of the public interest in access to and/or disclosure of data with IPRs in that data. As the *Geophysical* claim demonstrates, private rights in commercially valuable data can clash with the public interest. Particularly when it comes to confidential information, the public interest may be reflected in a broad range of laws and regulatory systems. The nature of the public interest may also change over time, especially as developments in technology increase the value of regulatory data. The *Geophysical* claim reveals both complex interests in data, as well as commercial needs for certainty and clarity when it comes to regulatory frameworks.

The burgeoning area of AI innovation relies on vast quantities of data, and AI governance schemes already attempt to address issues of bias in training data, as well as the use of personal data in automated decision making. In both cases, copyright and trade secret rights in these data could complicate AI governance regimes. This is particularly so if obligations in these areas expand without a concurrent expansion of the scope for exceptions in the public interest or a better articulation of the public interest in this context. A key challenge is to not overprotect data to the extent that there is no room for a broad understanding of the public interest. More important, perhaps, is the need to directly incorporate into international trade treaties scope for public interest considerations relating to data governance, particularly when linked to the protection of fundamental human rights.

Addressing public interest exceptions in the case of trade secret law may be particularly challenging. Trade secrets are different from other categories of IP. In many countries, there is no specific trade secret statute; indeed, in federal states, trade secret law – in contrast to copyright, patents, and trademarks – may not even be a matter of federal jurisdiction. Public interest exceptions to principles of confidentiality in many countries are scattered across a diverse range of law, including the laws of evidence, access to information laws, and various regulatory regimes. There is thus no international consensus, developed over time, on the nature and scope of needed exceptions.

Evolving negotiations regarding the protection of data as IP law must remain attentive to the complex range of public interests implicated by data, and the diffuse range of areas of law and policy which have long balanced confidentiality against broader public interests. They also should be attentive to the ways in which access to data, data transparency and data accountability may be required in order appropriately to govern artificial intelligence, to protect human rights, and to ensure goals of public safety and security.

REFERENCES

Aaronson, S A and T Struett (2020), "Data is Divisive: A History of Public Communications on E-commerce, 1998-2020", CIGI Papers No. 247, Centre for International Governance Innovation (www.cigionline.org/sites/default/files/documents/no.247_0.pdf).

Aggarwal, S (2018), "Treasure of the Commons: Global Leadership Through Health Data", Centre for International Governance Innovation (www.cigionline.org/articles/treasure-commons-global-leadership-through-health-data.

AI HLEG – High-Level Expert Group on Artificial Intelligence (2019), *Ethics Guidelines for Trustworthy AI*, European Commission (https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai).

Banterle, F (2016), "The Interface between Data Protection and IP law: The Case of Trade Secrets and Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis", in M Bakhoum, B Conde Gallego, M-O Mackenrodt and G Surblytė-Namavičienė (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?*, Springer, pp. 411-444.

Baron, J B (2012), "Property as Control: The Case of Information", *Michigan Telecommunication and Technology Law Review* 18: 367-418.

Bitton, M (2009), "Feist, facts and functions: historical perspective", in R F Brauneis (ed.), *Intellectual Property Protection of Fact-based Works: Copyright and Its Alternatives*, Edward Elgar, pp. 3-38.

Borgogno, O and G Colangelo (2020), "Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking", forthcoming in *Journal of European Consumer and Market Law* (http://dx.doi.org/10.2139/ssrn.3513514).

Casey, B, A Farhangi and R Vogl (2019), "Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise", *Berkeley Technology Law Journal* 34: 145–189 (https://btlj.org/data/articles2019/34_1/04_Casey_Web.pdf).

Centre for Information Technology, Society and Law (2017), "International Exploratory Workshop on Data Ownership" (www.itsl.uzh.ch/dam/jcr:1a3604c6-04b0-47ef-92a8-a329edf191ee/Workshop%20Summary.pdf).

Chander, A and U P Lê (2015), "Data Nationalism", *Emory Law Review* 64: 677-739.

Citron, D K and F Pasquale (2014), "The scored society: due process for automated predictions", *Washington Law Review* 89(1): 1-33 (https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2).

Congressional Research Service (2020), *Artificial Intelligence and National Security* (https://fas.org/sgp/crs/natsec/R45178.pdf).

De Filippi, P and S McCarthy (2012), "Cloud Computing: Centralization and Data Sovereignty", *European Journal of Law and Technology* 3(2) (https://ssrn.com/abstract=2167372).

Dennedy, M and S Leizerov (2017). "On monetizing personal information: A series", *The Privacy Advisor,* 26 September (https://iapp.org/news/a/on-monetizing-personal-information-a-series/).

Dickens, A (2020), "From Information to Valuable Asset: The Commercialization of Health Data as a Human Rights Issue", *Health and Human Rights Journal* 22(2): 67-70 (www.hhrjournal.org/2020/12/viewpoint-from-information-to-valuable-asset-the-commercialization-of-health-data-as-a-human-rights-issue/).

Drexl, J, R Hilty, L Desaunettes-Barbero, F Greiner, D Kim, H Richter, G Surblyte and K Wiedemann (2016), "Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate", Max Planck Institute for Innovation Competition Research Paper No. 16-10 (http://dx.doi.org/10.2139/ssrn.2833165).

Dusollier, S (2010), "Scoping Study on Copyright and Related Rights and the Public Domain", World Intellectual Property Organization (www.wipo.int/edocs/mdocs/mdocs/en/cdip_4/cdip_4_3_rev_study_inf_1.pdf).

Edwards, L and M Veale (2017), "Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for", *Duke Law Technology Review* 16(1): 18–84 (https://scholarship.law.duke.edu/dltr/vol16/iss1/2).

European Commission. (2020), "White Paper on Artificial Intelligence: a European approach to excellence and trust", COM(2020) 65 final (https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en).

European Medicines Agency (2014), "European Medicines Agency Policy on Publication of Clinical Data for Medicinal Products for Human Use" (www.ema.europa.eu/docs/en_GB/document_library/Other/2014/10/WC500174796.pdf).

Farkas, T J (2017), "Data Created by the Internet of Things: The New Gold Without Ownership?", *Revista La Propiedad Inmaterial* 23: 5-17.

Floridi, L, J Cowls, M Beltrametti et al. (2018), "AI4People — An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations", *Minds and Machines* 28(4): 689-707 (https://doi.org/10.1007/s11023-018-9482-5).

Furman, J and R Seamans (2019), "AI and the Economy", *Innovation Policy and the Economy* 19: 161-191 (www.journals.uchicago.edu/doi/10.1086/699936).

Gleeson, D, J Lexchin, J Labonté et al. (2019), "Analyzing the impact of trade and investment agreements on pharmaceutical policy: provisions, pathways and potential impacts", *Globalization and Health* 15(Suppl 1): 78 (https://doi.org/10.1186/s12992-019-0518-2).

Graef, I, J Verschakelen and P Valcke (2013), "Putting the Right to Data Portability into a Competition Law Perspective", *Law: The Journal of the Higher School of Economics, Annual Review* 2013: 53-63 (https://ssrn.com/abstract=2416537).

Hagen, G, C Hutchison, D Lametti, G Reynolds, T Scassa and M A Wilkinson (2018), *Canadian Intellectual Property Law: Cases and Materials* (2d edition), Emond.

Haupt, M (2016), "Introducing Personal Data Exchanges and the Personal Data Economy", Project 2030, 7 December (https://medium.com/project-2030/what-is-a-personal-data-exchange-256bcd5bf447).

Hill, J (2014), "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", The Hague Institute for Global Justice, Conference on the Future of Cyber Governance (https://ssrn.com/abstract=2430275 or http://dx.doi.org/10.2139/ssrn.2430275).

Hoeren, T (2014), "Big Data and the Ownership in Data: Recent Developments in Europe", *EIPR* 36(12): 751-754.

Hugenholz, B (2017), "Data Property: Unwelcome Guest in the House of IP", Paper presented at conference on "Trading Data in the Digital Economy: Legal Concepts and Tools", Münster (https://pure.uva.nl/ws/files/16856245/Data_property_Muenster.pdf).

Kerber, W (2018), "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", forthcoming in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (https://ssrn.com/abstract=3285240).

Kitchin, R (2014), *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences*, Sage Publications.

Lim, Y F (2018), *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*, Edward Elgar.

Liu, H-W and C-F Lin (2020), "Artificial Intelligence and Global Trade Governance: A Pluralist Agenda", *Harvard International Law Journal* 61: 407-450.

Lovell, T (2021), "Israel to share data with Pfizer in exchange for COVID-19 vaccine doses", *Health Care IT News*, 11 January (www.healthcareitnews.com/news/emea/israel-share-data-pfizer-exchange-covid-19-vaccine-doses).

MacGregor, I (2018), "Big Data: The Canadian Opportunity", CIGI, 5 March (www.cigionline.org/articles/big-data-canadian-opportunity).

McCann, D (2019), *e-Commerce Free Trade Agreements, Digital Chapters and the Impact on Labour: A comparative analysis of treaty texts and their potential practical implications*, The New Economics Foundation.

Mishra, N (2020), "International Trade Law Meets Data Ethics: A Brave New World", forthcoming in *New York University Journal of International Law and Politics* 43(2) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3689412).

Mishra, N (2019), "The Trade–(Cyber)security Dilemma and Its Impact on Global Cybersecurity Governance", forthcoming in *Journal of World Trade* (https://ssrn.com/abstract=3491122).

Morvan, A-S (2020), "A European Open Finance Framework by 2024" (http://dx.doi.org/10.2139/ssrn.3732405).

OECD (2015), "Approaches to the Protection of Trade Secrets", in *Enquiries into Intellectual Property's Economic Impact* (www.oecd.org/sti/ieconomy/KBC2-IP.Final.pdf).

Office of the National Counterintelligence Executive (2011), *Foreign Spies Stealing US Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (www.hsdl.org/?view&did=720057).

Patel, O and N Lea (2020), "EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows" (http://dx.doi.org/10.2139/ssrn.3618937).

Ravia, H, D Hammer and A Shoval (2021), "Israel Discloses its Agreement with Pfizer for De-identified COVID-19 Vaccine-related Health Data", 31 January (www.pearlcohen.com/israel-discloses-its-agreement-with-pfizer-for-de-identified-covid-19-vaccine-related-health-data/).

Ritter, J and A Mayer (2016), "Regulating Data as Property: A New Construct for Moving Forward", *Duke Law & Technology Review* 16: 220-277.

Scassa, T (2018), "Data Ownership", CIGI Papers No. 187 (www.cigionline.org/publications/data-ownership).

Scassa, T (2020), "Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto", *Technology Regulation Special Issue: Governing Data as a Resource*: 44-56 (https://techreg.org/index.php/techreg/article/view/51).

Schmelzer, R (2020), "Towards A More Transparent AI", *Forbes*, 23 May (www.forbes.com/sites/cognitiveworld/2020/05/23/towards-a-more-transparent-ai/?sh=1f682f693d93).

Shipley, D E (2007), "Thin But Not Anorexic: Copyright Protection for Compilations and Other Fact Works", *Journal of Intellecutal Property Law* 15: 91-141 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1076789).

Snower, D J and P Twomey (2020), "Humanistic Digital Governance", CESifo Working Paper No. 8792 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3754683).

Snower, D J, P Twomey and M Farrell, M (2020), "Revisiting Digital Governance", Social Macroeconomics Working Paper Series, Blavatnik School of Government (www.bsg.ox.ac.uk/sites/default/files/2020-10/SM-WP-2020-003%20Revisiting%20digital%20governance_0.pdf).

Thrasher, R D, V J Wirtz, W Kaplan, K P Gallagher and H Werk (2019), *Rethinking Trade Treaties and Access to Medicines Global Development Policy Center* (www.bu.edu/gdp/files/2019/11/Trade-Report-2019-GDP-Center-3.pdf).

Trakman, L, R Walters and B Zeller (2019), "Is Privacy and Personal Data Set to Become the New Intellectual Property?", *International Review of Intellectual Property and Competition Law* 50: 937-970.

UN Secretary-General's High-Level Panel on Access to Medicines (2016), *Promoting Innovation and Access to Health Technologies* (www.unsgaccessmeds.org/final-report).

Westerheide, F (2019), "The Artificial Intelligence Industry and Global Challenges", *Forbes*, 27 November (www.forbes.com/sites/cognitiveworld/2019/11/27/the-artificial-intelligence-industry-and-global-challenges/?sh=3c293ae3deb9).

Yakowitz Bambauer, J R and T Zarsky (2018), "The Algorithm Game", *Notre Dame Law Review* 94: 1-47 (https://ssrn.com/abstract=3135949).

Yu, P K (2018), "Data Exclusivities in the Age of Big Data, Biologics, and Plurilaterals", *Texas A&M Law Review* 6: 22-33 (https://ssrn.com/abstract=3133810).

ABOUT THE AUTHOR

Teresa Scassa is the Canada Research Chair in Information Law and Policy at the University of Ottawa, Faculty of Law. She is a member of the Canadian Advisory Council on Artificial Intelligence. She is the author of Canadian Trademark Law, and co-author of *Digital Commerce in Canada*, and *Canadian Intellectual Property Law*. She is a co-editor of the books *AI and the Law in Canada* and *Law and the Sharing Economy*. Her research interests include: privacy law, data governance, intellectual property law, law and technology, law and artificial intelligence, and smart cities.

CHAPTER 8

Asia-Pacific digital trade policy innovation

Stephanie Honey[1]
Honey Consulting Ltd.

INTRODUCTION

Digital technology is not just transforming trade in a multitude of ways, it is also prompting new policy and regulatory responses from governments – at a pace that far outstrips the normal rhythms of trade policymaking. These governmental responses may create new impediments to digital trade but also serve as a potential means to address them – no more so than in the Asia-Pacific region. Asia-Pacific economies are at the forefront of global technological innovators, digital businesses and digitalised communities; unsurprisingly they have also been in the vanguard of digital trade policymaking. Many Asia-Pacific free trade agreements (FTAs) already include ambitious e-commerce chapters. More recently, 'digital first' approaches take a broad view of the cross-border digital economy and emphasise cooperation and agility in seeking to regulate it.

These more agile and collaborative approaches are better suited to digital trade than the rigidities of more traditional trade policymaking, given the relatively fast pace of change in technology and associated business models. Cooperative and responsive trade policy models can serve as useful building blocks to the eventual creation of broader multilateral 'hard law' outcomes. Indeed, multilateral rules would be the optimal end-point for a form of trade that is in many ways borderless, which is increasingly dominant around the globe, and where expanding trade restrictions threaten to reduce the economic value that can be realised from the digital economy.

THE DIGITAL TRANSFORMATION OF TRADE

Even as far back as 2014, the economic value of cross-border data flows was estimated to have superseded that of trade in goods, with data flows growing exponentially and predicted to add trillions to global GDP in the coming decade (Manyika et al. 2016). Rates of growth of the digital economy overall, and exports of digital services – including computer and IT services along with those in other digitally enabled sectors such as

1 The views expressed in this chapter are entirely those of the author in a personal capacity and do not necessarily reflect the views of any of her other professional affiliations.

publishing, audio-visual services and telecommunications – have far outstripped broader economic growth in recent years, with 'digital-based globalisation' expanding just as more traditional manufacturing-based pathways are in decline (van der Marel 2020).

The transformative impact of digital trade is not just about the numbers, however, but the remodelling of trade itself. Data can itself be a traded, and cross-border data flows are also driving the 'servicification' of manufacturing, and even the transformation of physical goods into services. Data flows enable the unbundling of production processes into global value chains, underpin a significant and growing share of the services that are able to be supplied across borders, and unlock substantial reductions in the trade costs of even traditional sectors such as agriculture. At the same time, big data analytics and digitally enabled supply-chain traceability are creating new opportunities for value-adding, for example through tailoring product offerings and enabling market positioning based on verifiable product attributes (Baldwin 2016, 2019, United Nations 2017).

This is not a static situation. Emerging 'enabling' technologies, including artificial intelligence (AI) and automation, digital identities, blockchain, additive manufacturing and the Internet of Things (IoT), have the potential to reduce costs and add value to other kinds of trade. One forecast suggests that by 2030, AI could increase global economic output by US$13 trillion, and we may see an increasingly disruptive impact on business and trade in coming years (Bughin et al. 2018). As for the IoT, over 20 billion devices are already connected to the internet; by 2030 that number is estimated to be 50 billion – nearly six for every person on the planet – all enabled by data flows, including across borders.[2]

The case for accelerating work on digital trade rules could scarcely have been made more compellingly than by COVID-19. The pandemic has demonstrated just how essential digital technologies now are for doing business at home and across borders. Although overall commercial services trade saw a steep decline in 2020, computer services (as just one component of 'digital trade') grew substantially, increasing by 9% in the third quarter relative to 2019 figures (WTO 2021). The number of internet users in 2020 increased by over 7%, social media by half a billion users, and e-commerce expanded by double figures in consumer categories such as food, clothing, music and videogames (Hootsuite and We Are Social 2021).

As countries start to turn towards post-COVID rebuilding, digital trade also has an important role to play in economic recovery – including for small businesses, women, and other groups which have traditionally struggled to take advantage of trade opportunities, but for which digital trade offers a springboard to foreign markets. The smallest of firms, so-called 'micro-multinationals', can already compete on the global stage at minimal cost. Emerging and developing economies may be able to leapfrog some of the more traditional trade structures. Even businesses which are exclusively focused on domestic markets

2 https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

make use of digitally traded inputs, for example through cloud computing and other imported digital back-office, production-related or distribution services. The OECD says that greater accessibility of digital trade can contribute to speeding up economic recovery (OECD 2020).

In the period ahead, we are likely to face an ongoing downside risk from the pandemic and a stuttering global economy (IMF 2021). Based on the evidence to date, this may also generate ongoing pressures for greater economic nationalism, including in the digital economy. For example, even where COVID had accelerated the transition to more digital models such as the use of e-signatures and electronic documentation in response to outbreaks and social distancing requirements, we are seeing countries reverting to an insistence on paper documents.[3] This reversion to traditional approaches may be being driven by protectionist motives.

Given the complexity of the digital economy, the scope and implications of relevant regulation may not be immediately apparent, including for businesses seeking to operate across borders. This points strongly to creating greater certainty through new trade rules – recalling that trade agreements have traditionally served to provide transparency, predictability and to at least some degree a more level playing field, and those things continue to matter, especially for small and medium-sized businesses and small economies. In short, digital trade rules will need to be fit for purpose in the face of a range of impediments and to realise opportunities – and this points to a need to step up progress in developing and refining digital trade governance.

IMPEDIMENTS TO DIGITAL TRADE

There is no globally agreed definition of 'digital trade', and accordingly no agreement on the scope of possible impediments to digital trade, nor indeed on what constitutes 'digital protectionism'. The OECD has provided a useful starting point, defining digital trade as "digitally enabled transactions in trade in goods and services, whether digitally or physically delivered" (López Gonzalez et al. 2018). Such a definition captures forms of trade that are entirely 'digital' (for example, the provision of digital media via a streaming service that is consumed online) as well as online-to-offline forms, such as goods that are digitally ordered but physically delivered using an e-commerce platform.

However there is a strong case to be made for using a broader definition than this, one that in addition captures how data flows enable digital trade through the cross-border movement of data itself as a traded product, or through the productivity gains from using digital services that make firms more competitive domestically and overseas (Meltzer 2019). Equally, given the rapid pace of digital transformation, it can be argued that the definition itself may need to be reviewed and updated over time, for example to take

3 https://www.unescap.org/news/trade-and-investment-indispensable-post-covid-recovery-asia-and-pacific-un-meeting-says

account of how frontier technologies such as AI may interact with trade. These broader conceptualisations of 'digital trade' go beyond the scope of many of the e-commerce chapters in trade agreements to date.

A lengthy catalogue could be compiled of potential impediments to digital trade. The most salient relate to data flows, and the different categories of restrictions used on the movement of data across borders (or in trade agreements language, "cross-border transfer of information by electronic means") and on its storage and processing (that is, "location of computing facilities") (Meltzer and Lovelock 2018, Ferracane 2017). Data flow regulations can be designed to address a range of public policy objectives including privacy, cybersecurity, consumer protection, cybercrime or censorship of content – or in some cases, for outright protection of domestic economic interests. Even where the stated policy goals may be legitimate, however, the design of measures may go further than necessary to meet the objective or might impose a disproportionate or disguised restriction on trade.

The level of restriction arising from data flow regulations including data localisation measures can be considerable for particular types of services or sectors, according to the OECD's Digital Services Trade Restrictiveness Index (OECD 2020). In turn, the impact of such restrictions on GDP, domestic investment and economic welfare overall can be significant (van der Marel et al. 2014). The impact at the individual firm level can be much more difficult to measure – but business surveys suggest that data-related restrictions are seen by business as a significant impediment to, or at least an additional cost on, doing business in the region, and can have an impact on innovation and productivity (ABAC 2019).

Beyond data-related restrictions, a range of other impediments to digital trade can be identified. These can include measures relating to intellectual property rights, divergent or proprietary standards, or filtering or blocking of certain sites or content (Aaronson 2019). For digital services providers, barriers can include those that affect more 'traditional' services trade such as market access limitations, discriminatory licensing or commercial presence requirements, as well as a host of impediments specific to the provision of particular digital services, notably those relating to e-payments, such as discriminatory access to online payments, restrictions on internet banking or insurance and lack of international standards for e-payments (OECD 2020). There are also ongoing pressures for imposing customs duties on electronic transmissions (Wu 2017); and in the last few years, there has been increasing pressure for taxation of cross-border digital services suppliers.

Likewise, the competitive environment needs to be considered. For exporters of physical goods and some digital services such as gaming or streaming of music or video, for example, while platform-based trade offers some significant advantages of reach, streamlined costs

and payment facilitation, especially for small businesses, the market power of platforms and biases in or lack of transparency around the algorithms that underpin them may ultimately also act as an impediment to digital trade.

Finally, in relation to the nexus between digitally enabled trade and traditional physical goods exports, there may be procedural obstacles and physical chokepoints as the small parcel-based trade of e-commerce confronts the limitations of existing border infrastructure and administrative procedures (Meltzer 2019). In short, the list of barriers to digital trade is a long one.

It is also clear that tackling impediments to digital trade is not simply about removing barriers, but also focusing on shoring up 'enablers' of trade, particularly to empower small businesses to take advantage of digital transformation. In the case of some tools for digital trade facilitation, for example, such as electronic trade documentation or blockchain-based supply chain management, or emerging technologies such as AI, interoperability across both the technical standards and regulatory or legal layers may be necessary to enable greater cross-border uptake.

BUSINESS PERSPECTIVES ON THE DIGITAL LANDSCAPE

Research into business perspectives in the Asia-Pacific in recent years confirms that business is indeed challenged by many of the impediments identified in the literature discussed above, including data-flow restrictions, commercial presence requirements, restrictive policies on fintech (including around accepting and processing payments and tax policies), intellectual property protection measures, procedural obstacles at the border for platform-based goods trade, and issues relating to accessing global e-commerce platforms (ABAC 2019, ABAC 2015). Businesses also highlight constraints on accessing the requisite 'talent' for technology firms (for example through cross-border Mode 4 services supply), especially since in some cases the talent concerned does not fit standard professional categories (ABAC 2018).

However, in terms of priorities, the research also suggests that one of the major concerns for businesses in the region is simply the increasingly complex, ambiguous and heterogeneous regulatory environment that the participants in digital trade must navigate. In one research survey, 76% of businesses identified inconsistent regulations and standards as the most important barriers to digital trade (ABAC 2019). In another, 79% identified the quality and enforcement of laws and regulations as a problem; and in another, 56% identified non-interoperability of digital systems as a 'major' or 'severe' problem (ABAC 2015, ABAC 2018).

In other words, business is struggling with an emerging 'digital noodle bowl'[4] of divergent regulations on digital trade. Differences in regulation across markets are a major challenge for a business model that in many cases is effectively 'global' rather than market-specific, especially where cross-border data flows are a major component of that model. Businesses that were surveyed also identified a lack of readily accessible information about trade requirements and inadequate digital capability, especially among small businesses, as serving as an impediment to trade, with 46% identifying 'ambiguity of regulations' as a problem in one survey (ABAC 2019).

The research also throws up some interesting nuances between what are perceived as 'impediments' by businesses and those identified by economists or policymakers. For example, the research suggests that businesses can struggle with the high compliance costs associated with some forms of privacy regulation, while nevertheless fully recognising the value and importance of privacy regulation per se, both because of the priority they attach to the protection of data for the integrity of their businesses, well as to shore up their social licence to operate by fostering consumer trust. In that regard, where to draw the line between 'legitimate' restrictions and those that add unwarranted or disproportionate costs can be complex and challenging (Aaronson 2019).

In other cases, for example around data localisation or transfer of source code, these requirements may be elements in commercial contracts (as well as or instead of regulated requirements), and so may be less readily identified by businesses as 'trade' barriers; or businesses may simply seek a workaround, for example by licensing a local partner rather than establishing a local server.

In fact, as the discussion above suggests, one of the challenges for trade negotiators that this research underscores is that the impact of many of these measures may be subtle or opaque, and businesses may not necessarily identify them as 'trade barriers' – rather, seeing them as 'just the cost of doing business'. This perception may make it difficult for policymakers to engage effectively with businesses to catalogue the full range of impediments to digital trade that they may encounter and consequently to develop effective approaches in mitigation. Arguably, perhaps the current models of stakeholder engagement still owe too much to the 20th century mindset where 'trade' comprises goods, services and investment, rather than one updated for the digital 21st century and sensitive to a more ambiguous range of trade barriers and diverse stakeholders.

4 Bhagwati (1995) originally coined the term 'spaghetti bowl' to describe overlapping and potentially divergent rules of origin across trade agreements, but this was subsequently characterised as a 'noodle bowl' in Asia (e.g. Kawai and Wignaraja 2009).

FTA APPROACHES: ASIA-PACIFIC INNOVATION

Free trade agreements are currently the main vehicle for digital trade policymaking. This has led to a patchwork of different rules around the world, including 182 preferential trade agreements (PTAs) with provisions relating to digital trade, 107 PTAs with specific e-commerce provisions and 77 with dedicated e-commerce chapters, out of 345 PTAs concluded between 2000 and June 2019 (Burri and Polanco 2020).

Two of the three major 'templates' among these PTAs – the US approach and that of China – are to be found in the Asia-Pacific. In fact, the Asia-Pacific region is in the vanguard of digital trade policy-making in general, with a web of successive overlapping agreements that include digital provisions, as well as an ongoing workstream to explore the policy implications of the digital economy in the Asia Pacific Economic Cooperation (APEC) forum, which includes 21 of the region's major economies.[5]

This strong focus on digital trade is not surprising, given the predominance of large technology companies, mobile-first consumers and digital norm-setters in the region – although there is also significant divergence in governance models, especially between the US and China (Aaronson and Leblond 2018). This web of Asia-Pacific agreements has had mixed success in tackling impediments, but some of the more recent of these have used innovative approaches to address not just barriers to digital trade, but a wide range of enablers as well.

The evolution of digital trade policymaking in the Asia-Pacific

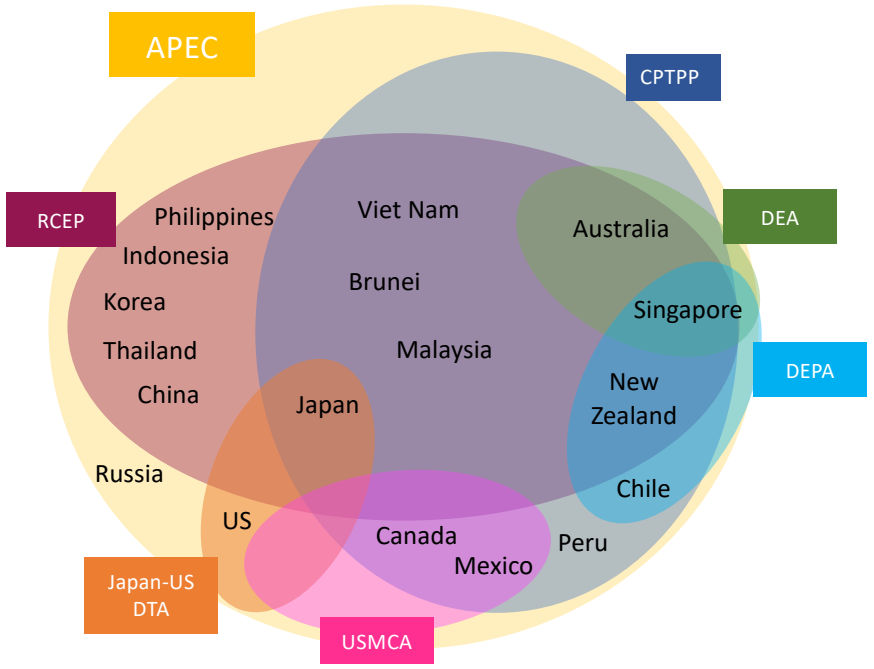
Some of the earliest specific digital trade provisions in the world are to be found in the region, starting with the Singapore-New Zealand Closer Economic Partnership Agreement of 2000, with provisions on paperless trading and on the transfer of financial information and data processing (Burri and Polanco 2020). In 2003, the first regional trade agreement to include an explicit standalone chapter on e-commerce was the FTA between Australia and Singapore, closely followed by four more intra-Asia-Pacific regional agreements with e-commerce chapters involving Australia, Singapore, the United States or some combination thereof, and in 2008 the ASEAN-Australia-New Zealand FTA (AANZFTA) (Wu 2017).

A path can be traced from those earliest provisions through to the Trans-Pacific Partnership Agreement in 2016, which by 2018 had become the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), somewhat modified in places, although not in the e-commerce chapter. Subsequently, regional agreements have drawn on the CPTPP template, including the Chile–Uruguay FTA (2016), Singapore–Australia FTA (2016), Argentina–Chile FTA (2017), Singapore–Sri Lanka FTA (2018),

5 The APEC member economies are: Australia; Brunei Darussalam; Canada; Chile; China; Hong Kong, China: Japan; Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Philippines; Russia; Singapore; Chinese Taipei; Thailand, United States, Viet Nam.

Australia–Peru FTA (2018), and Australia–Indonesia FTA (2019), as well as the more ambitious United States–Mexico–Canada (USMCA) agreement (2018) and the Japan–US Digital Trade Agreement (2019) (Burri 2020). Ultimately, the path leads to the Digital Economy Partnership Agreement (DEPA), and the Australia–Singapore Digital Economy Agreement (DEA), in mid-2020. The overlapping membership of a number these agreements is set out in Figure 1 below.

FIGURE 1 THE OVERLAPPING WEB OF DIGITAL TRADE RULES IN THE ASIA-PACIFIC: A REPRESENTATIVE (NON-EXHAUSTIVE) SELECTION OF AGREEMENTS



Notes: CPTPP is the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018), DEA is the Digital Economy Agreement (2020), DEPA is the Digital Economy Partnership Agreement (2020), APEC is Asia Pacific Economic Cooperation, USMCA is the United States-Mexico-Canada Agreement (2020), Japan-US is the Japan-US Digital Trade Agreement (2020), RCEP is the Regional Comprehensive Economic Partnership agreement (2020).

Source: Author.

In broad-brush terms, the Asia-Pacific FTAs described above take a similar, but progressively more ambitious and expansive approach, seeking to remove impediments to digital trade primarily by addressing data flows and governance, along with digital enablement of more traditional forms of trade as well as trade through digital channels such as e-commerce platforms. These agreements include provisions on domestic regulatory frameworks, data governance and trust (including provisions on transparency, online consumer protection, data regulation, and, in the later agreements, data protection,

privacy and cybersecurity); digital trade facilitation measures (including provisions on paperless trade, electronic authentication, digital certificates and in the later agreements a host of more detailed provisions); and cooperation undertakings.

New Zealand and Singapore – along with 14 other economies in the region (the ten ASEAN countries, China, Japan, Korea and Australia) – are also part of the Regional Comprehensive Economic Partnership (RCEP) agreement, signed at the end of 2020. Although this agreement clearly shares the lineage of earlier Asia-Pacific e-commerce chapters, its approach to data in particular is somewhat different, as is discussed further below.

The CPTPP template and RCEP divergence on data governance

The approach to data flows has evolved substantially since those first provisions in the 2000 Singapore–New Zealand agreement. In the 2006 AANZFTA agreement among ASEAN, Australia and New Zealand, for example, a Party was only obliged to protect personal data "in a manner it considers appropriate" (and even then, not until it had enacted its own relevant laws or regulations domestically); dispute settlement did not apply to the electronic commerce chapter.[6] By the 2018 CPTPP, by contrast, members were *required* to have in place domestic data protection regimes.[7]

On data flows, CPTPP guarantees that "[e]ach Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person". Exceptions are permitted only to meet "legitimate objectives", provided that they do not "amount to arbitrary or unjustifiable discrimination or a disguised restriction on trade".[8] (Note also that the definition of covered person excludes financial institutions and cross-border financial services suppliers).[9]

CPTPP also prohibits forced data localisation, with a similar exception for legitimate public policy objectives as is provided for data flows. [10] In practice, this has enabled a degree of policy flexibility – for example, in Viet Nam's recent Cybersecurity Decrees, which require domestic internet service providers to store all data originating within Viet Nam for at least 15 days, and which also impose data localisation requirements on over-the-top service providers (that is, media services offered directly to consumers over the internet, such as video streaming).[11]

6 ASEAN-Australia-New Zealand FTA, 2008, Chapter 10, Art. 7.
7 CPTPP Chapter 14.
8 CPTPP, Art. 14.11.
9 CPTPP, Art. 14.1
10 CPTPP, Art. 14.13.
11 CPTPP, Art. 14.13; example cited in Meltzer (2019: s36).

By contrast, RCEP – which has a seven-member overlap with CPTPP[12] – provides for far more 'policy space' on data flows and data storage requirements. While it has provisions along CPTPP lines specifying free flows of data and a prohibition on localisation, it allows for significantly wider exceptions than does CPTPP.

Specifically, while RCEP members have agreed that they "shall not prevent cross-border transfer of information by electronic means…", but also that, "[n]othing in this Article shall prevent a Party from adopting or maintaining: (a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties."[13]

Similarly, on data localisation, RCEP provides for an exception to the prohibition on data localisation under which a Party can impose any measure "necessary for the protection of its essential security interests", making clear that the "legitimate public policy objective" exception can be decided solely by the implementing Party.[14] No definition is provided for "essential security interests" (and note that this not even qualified as being "*national*" security interests), nor any guidance on the application of the necessity test.

In other words, as long as data flow restrictions and data localisation requirements are not applied in a discriminatory way, RCEP members may impose them; and even discriminatory approaches may be permitted if they are necessary, in the view of the country concerned, for the protection of its essential security interests. In either case, the dispute settlement provisions do not apply. This potentially creates significant room for restrictive data requirements among RCEP members. In practice, how far RCEP members will use this 'policy space', including to maintain or create new impediments to digital trade, remains to be seen. It is worth bearing in mind that RCEP is the world's largest FTA, measured in terms of participants' GDP.[15]

Also unclear is the interplay between the potentially more restrictive RCEP data rules, and those in CPTPP, for the seven countries that are party to both agreements. Article 20 of RCEP provides that if a Party considers a provision of the agreement to be inconsistent with another agreement, the relevant Parties will consult with a view to reaching a mutually satisfactory solution. However, potentially there could be 'duelling rulebooks' for digital trade among those seven overlapping members.

12 New Zealand, Australia, Japan, Singapore, Malaysia, Viet Nam and Brunei are all members of both RCEP and CPTPP.
13 RCEP, Art. 12.15
14 RCEP Art. 12.14
15 RCEP's members have a combined GPD of around $25.8 trillion; USMCA $24.4 trillion, EU $18.9 trillion and CPTPP $13.5 trillion. Felix Richter, RCEP: Asia-Pacific Forms World's Largest Trade Bloc', Statista, 16 November 2020.

Nevertheless, there are still reasons to welcome the RCEP provisions in terms of their contribution to regional data governance, foremost among which is that China is a member of the agreement. As noted above, China has usually taken a very different approach on data than the CPTPP model (Aaronson and Leblond 2018). By contrast, in RCEP, China has agreed that the default should be free flows of data and no forced data localisation, albeit with a potentially broad exceptions provision. Even if in practice the exceptions become the binding constraint , RCEP nevertheless creates a forum for an ongoing conversation on data flows, data localisation, source code and the treatment of digital products in a formal Dialogue on Electronic Commerce among the Parties.[16] This dialogue may eventually help to narrow the scope of exceptions (and hence potential impediments to digital trade) in the future.

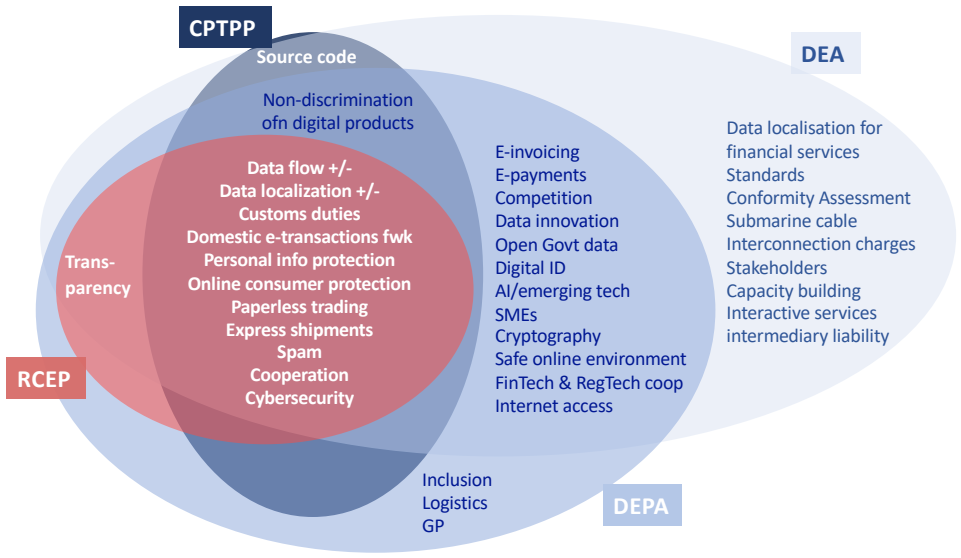
DIGITAL TRADE POLICY INNOVATION: DEPA AND DEA

Two very recent agreements, both concluded in mid-2020, take a broader approach to digital trade than either CPTPP or RCEP: the Digital Economy Partnership Agreement (DEPA) and the Digital Economy Agreement (DEA). DEPA is a standalone agreement involving New Zealand, Singapore and Chile. (Chile has yet to ratify the agreement, although it entered into force for New Zealand and Singapore in January 2021). The DEA between Singapore and Australia is in fact an amendment to the existing Singapore–Australia FTA of 2015. There are also seven DEA-linked Memoranda of Understanding which identify or map collaboration projects on AI, data innovation, digital identities, personal information protection, e-invoicing, trade facilitation and e-certification for agriculture.[17]

While their core elements closely reflect CPTPP provisions, these new agreements go considerably further in terms of scope, and – in a number of key elements – in ambition. On scope, this broadening reflects a wider conception of what constitutes 'digital trade': where CPTPP governs measures that "*affect trade by electronic means*", DEPA by contrast includes measures that "*affect trade in the digital economy.*"[18] Consequently the range of issues covered by DEPA and DEA is far broader than CPTPP, encompassing not just issues relating to data flows and digital trade facilitation, but also subjects as diverse as emerging technologies, innovation, and inclusion. Figure 2 illustrates this broadening of scope.

16 RCEP, Section E, Art. 12.16
17 Australian Department of Foreign Affairs and Trade (www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement).
18 DEPA, Module 1, Art. 1.1.1; CPTPP, Art. 14.2.2; see also DEA Annex A, Art 2.1.

FIGURE 2 TOPIC COVERAGE IN CPTPP, RCEP, DEPA AND DEA



Source: Author

While broader than CPTPP in some ways, because it is 'digital only', DEPA does not include chapters that could be found in a comprehensive FTA, such as services market access and rules on intellectual property (IP) and technical barriers to trade. These clearly have a significant bearing on impediments to digital trade (for example, through opening up market access for digitally-delivered services, or removing or introducing limitations on IP protection), and in that sense, DEPA falls short of what could potentially be achieved in a more comprehensive FTA – but equally it also addresses impediments that fall outside of these 'traditional' FTA chapters. At least as far as the three current three participants are concerned, the more comprehensive FTAs to which they are already mutually Parties, notably CPTPP, include those other elements. Should DEPA membership be broadened (as is the intention), the omission of services market access and other rules may become a more pressing concern in terms of addressing impediments to digital trade in the DEPA 'zone'.

The broader context for digital trade in DEPA and DEA

While both DEPA and DEA are aimed at fostering the trade and economic opportunities arising from the digital economy, they also clearly situate digital trade in broader socioeconomic context. This may have the effect (or at least be intended to have the effect) of addressing structural impediments that may otherwise prevent the uptake of digital trade opportunities, as well as preserving policy space for governments in areas that have a bearing on the digital economy. In the DEPA preamble, for example, the Parties "reaffirm the importance of promoting corporate social responsibility, cultural identity

and diversity, environmental protection and conservation, gender equality, indigenous rights, labour rights, inclusive trade, sustainable development and traditional knowledge, as well as the importance of preserving their right to regulate in the public interest".

Subsequently this preambular language is put in more operative terms with substantive provisions on "Inclusion" (including indigenous communities, women and rural populations) and "Small and Medium-sized Enterprises" (SMEs). These modules include best-endeavours provisions to enable the participation of those identified groups in the digital economy.[19] DEA likewise has an article on SMEs along similar lines, and also includes cooperation on regional capacity building.[20]

How much practical effect these provisions will have is as yet untested. Similarly, the interplay of the provisions on inclusion with other relevant international instruments is not yet clear – for example, in the case of the DEPA provisions on indigenous peoples, this may throw up a range of complex issues, including around indigenous data sovereignty, as and whether the agreement intersects with the UN Declaration on the Rights of Indigenous Peoples.

Both DEPA and DEA also have provisions on "Online Safety and Security", with DEPA recognising "the importance of taking a multi-stakeholder approach" to addressing the issues and agreeing to "endeavour to cooperate to advance collaborative solutions", and DEA recognising the need to address "harmful content, including terrorist and violent extremist content" and noting the "shared responsibility between governments, technology service providers and users" for online safety, with Parties agreeing to "endeavour to maintain an open, free and secure Internet".[21] While only at an early stage of policy development, the inclusion of the provisions at all is a departure from CPTPP.

Collaboration and agility – and the role of business

Another feature of these agreements is an emphasis on policy flexibility and responsiveness; in short, DEPA and DEA recognise that the development of technology and the associated business models have far outpaced the regulatory approaches in this area, and that this mismatch in speed is likely to continue. Fundamental to DEPA, accordingly, is the concept that it is a living agreement in which policymakers must respond to a rapidly evolving landscape. The preamble states that the Parties "acknowledge that the digital economy is evolving and therefore this Agreement and its rules and cooperation must also continue to evolve", and one of the functions of a newly-constituted DEPA Joint Committee, consisting of government representatives of each Party, is to "consider ways to further enhance the digital economy partnership between the Parties."[22]

19 DEPA, Preamble; and Module 11.
20 DEA, Art. 36 and 37.
21 DEPA, Module 5, Art. 5.2; DEA Art.18
22 DEPA, Preamble and Module 12.

There are also undertakings in both agreements to cooperate to advance collaborative solutions, such as regulatory sandboxes and ongoing dialogue on a range of topics, including data innovation, AI, digital identities, fintech and standards.[23] While many of these provisions on collaboration are only aspirational, they may eventually move from soft norms to binding 'hard law' as the policy and economic implications of these new technologies (and the appropriate regulatory responses) become more clear.

A key component of both agreements is also close engagement with the business community, academics and technical experts, reflecting the fact that designing good policy in this area of the economy – perhaps more than for any other – calls for a degree of technical or specialist expertise, which can be found among the tech or business sector itself. DEPA sets up a Digital SME Dialogue including the private sector, non-governmental organisations, academics and others stakeholders, and notes that, "[t]he Parties may consider using relevant technical or scientific input, or other information arising from the Dialogue, towards implementation efforts and further modernisation of this Agreement". DEA has similar provisions in its article on Stakeholder Engagement, and likewise sets up a Digital Economy Dialogue including researchers, academics and industry.[24]

As discussed above, there may be challenges for policymakers in gaining substantive inputs on trade barriers from stakeholders, given that businesses may not necessarily perceive the issues through a 'trade' lens, though they may be more familiar with the technological elements involved than the policymakers themselves. At the least, however, these dialogues may help to address the impediment identified in business surveys of a lack of accessible information about digital economy regulation.

Greater ambition than CPTPP in places…

In their core elements, including data flows and data localisation, DEPA and DEA reflect the CPTPP template, but go further in reducing potential impediments to trade compared with CPTPP in a number of areas. Foremost among these are paperless trade, domestic electronic transactions frameworks, cybersecurity and transparency, where the DEPA and DEA provisions add considerably more detail and/or operative language, and are likely to deliver practical improvements in the cross-border operating environment for businesses. Table 1 sets out a non-exhaustive list of provisions in CPTPP, RCEP, DEPA and DEA, and in very broad-brush terms their relative level of ambition.

23 For example, DEPA, Module 7, 8, 9; DEA Art. 26, 29, 30.
24 DEPA, Module 10; DEA Art. 37.

TABLE 1 COMPARISON OF DIGITAL PROVISIONS IN CPTPP, RCEP, DEPA AND DEA

Digital trade provisions	(CP)TPP 2016/18	RCEP 2019	DEPA 2020	DEA 2020
No Customs duties on electronic transmissions	Y	Y	Y	Y
Non-discrimination on digital products	Y	N	Y	Y
Domestic electronic transactions framework	Y	Y-	Y+	Y
Personal information protection	Y	Y--	Y+	Y
Electronic authentication/signatures	Y	Y	N	Y+
Online consumer protection	Y	Y	Y	Y
Paperless trading	Y	Y	Y++	Y+
Express shipments	Y	In FTA	Y	Y
Electronic invoicing	N	N	Y-	Y+
Electronic payments	N	N	Y	Y
Data flow	Y	Y--	Y	Y
Data localisation	Y	Y--	Y	Y
Data localisation for financial services	N	N	N	Y
Unsolicited commercial e-messages	Y	Y	Y	Y+
Cooperation	Y	Y	Y	Y
Cooperation on competition policy	N	N	Y	Y
Cybersecurity	Y	Y	Y+	Y+
Dispute settlement	Y	Y	Y+	In FTA
Transparency	N	Y	Y+	Y
Source code	Y	N	N	Y+
Data innovation	N	N	Y	Y
Open government data	N	N	Y	Y-
Digital identities	N	N	Y	Y+
Emerging technologies/artificial intelligence	N	N	Y	Y+
SMEs	N	N	Y+	Y
Cryptography	N	N	Y	Y
Creating a safe online environment	N	N	Y-	Y+
FinTech and RegTech cooperation	N	N	Y	Y+
Access to the internet	N	N	Y	Y
Inclusion	N	N	Y	N

Digital trade provisions	(CP)TPP 2016/18	RCEP 2019	DEPA 2020	DEA 2020
Logistics	N	N	Y	N
Government Procurement	N	N	Y-	N
Institutional arrangements	N	N	Y+	N
Standards & conformity assessment	N	N	N	Y
Interactive services intermediary liability	N	N	N	Y
Submarine Cable	N	N	N	Y
Interconnection Charges	N	N	N	Y
Stakeholder Engagement	N	N	N	Y
Capacity-building in the region	N	N	N	Y

Notes: Y = provision is similar or identical across agreements, from the CPTPP 'baseline'; Y+ = Provision is more comprehensive and/or ambitious; Y- = Provision is less comprehensive and/or ambitious; N = No similar provision included.

On personal information protection, for example, DEPA goes further than the best-endeavours language of CPTPP, explicitly requiring the adoption of non-discriminatory practices in protecting users of e-commerce from privacy violations. DEPA Parties are also obliged to pursue mechanisms to "promote compatibility and interoperability" between different privacy regimes (as opposed to simply "encouraging the development" of such mechanisms), and the agreement sets out a list of the principles which should underpin a robust privacy framework.[25] DEA takes a slightly different approach, calling for the use of the APEC Cross-Border Privacy Rules, a mechanism that enables interoperability of privacy regimes across different jurisdictions for accredited firms. Both DEPA and DEA also encourage the use of data trustmarks – again, with emphasis on practical business needs.[26]

Similarly, DEA takes a more ambitious approach than CPTPP by explicitly including financial services in the prohibition on forced data localisation. This expansion of the CPTPP coverage is enabled by a qualification that requires that, for financial services, authorities have "immediate, direct, complete and ongoing access to information processed or stored on computing facilities that the covered financial person uses or locates outside the Party's territory" – a practical solution to mitigate possible concerns around both prudential requirements and cybercrime that may arise in respect of cross-border trade in financial services, while preserving the default prohibition on forced data localisation.[27]

25 DEPA Module 4, Article 4.2; the list of principles is: collection limitation, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability. Compare with CPTPP Art. 14.8.
26 DEPA Module 4, Art. 4.2; DEA Art. 17.
27 DEA, Art. 25.

This 'solution' could also point to a possible way forward on concerns in other settings or agreements around access to data for law enforcement purposes, which can be a problem both domestically and cross-border and for which current legal processes are both cumbersome and time-consuming (Meltzer and Lovelock 2018).

… and broader scope than CPTPP, too

DEPA has a 'modular' design, with 16 modules on a diverse range of topics – reflecting, as noted above, a fundamentally broader definition of what relates to 'digital trade', and hence the agreement's ability to tackle potential barriers to that trade. A number of the elements covered by individual modules, as well as elements within other modules, were not included in CPTPP, including electronic invoicing, electronic payments, cooperation on competition policy, data innovation and open government data, digital identities, emerging technologies including artificial intelligence and fintech, and logistics and cryptography.

The scope of DEA is broadly similar. It does not include some DEPA topics (such as inclusion, logistics or government procurement), but on the other hand brings in a number of other elements including articles on standards and conformity assessment, stakeholder engagement, capacity-building and submarine telecommunications cable systems. In some shared areas, DEA goes further than DEPA, with more operative provisions rather than simply best-endeavours language – for example, on e-invoicing, digital identities and artificial intelligence, but in other areas, such as paperless trading, privacy, competition policy, SMEs and transparency, DEPA goes further.

Standards and interoperability: The next frontier of digital trade barriers

One important area where these agreements break new ground relates to international standards. As in more traditional trade models, divergent or inconsistent national standards can act as non-tariff barriers or impediments to digital trade; and equally, coherent, harmonised or mutually recognised standards can serve as important enablers of trade (TRPC 2020). In traditional FTAs, of course, this is addressed through chapters on technical barriers to trade that seek to streamline technical requirements and minimise divergences, including through recourse to international standards. However, the body of international standards in the digital economy is far more modest than for traditional trade. Equally important in the digital economy are the legal and regulatory settings that allow for digital technologies (such as legal validity of e-documents or e-signatures).

Both DEPA and DEA refer throughout to the development, use and compatibility or interoperability of standards. In its preamble, for example, the DEPA Parties "recognise the role of standards, in particular open standards, in facilitating interoperability between digital systems and enhancing value-added products and services".[28] DEA goes further,

28 DEPA, Preamble.

including a detailed standalone Article on "Standards and Conformity Assessment for Digital Trade". DEA also has a strong emphasis on the compatibility of standards, the development of common standards, and the use of international standards, for example in provisions on e-invoicing, e-payments, digital identities, AI, fintech and data portability.[29]

Where DEA emphasises "compatibility", however, DEPA has a stronger emphasis on "interoperability". This likely reflects the open nature of DEPA; interoperability implies that coherence can be achieved even when standards or systems are technically different – including through mechanisms such as application programming interfaces (for, example for e-payments systems) – whereas compatibility implies a more forced convergence around systems or standards. In a practical sense, interoperability is likely to be more achievable in the short term than compatibility or harmonised approaches.

For example, on digital identities, New Zealand is currently developing its approach through a new Trust Framework and is considering models including decentralised digital identities, whereas by contrast Singapore has an existing national (centralised) scheme. DEPA brings the two together by mandating collaborative work to develop mechanisms and frameworks for the interoperability of digital identity systems in the technical, security and legal/regulatory layers as well as in policy settings.[30]

DEPA acknowledges the role of digital identities in regional and global connectivity, recognises that digital identity can be individual or corporate, and acknowledges that the legal or regulatory frameworks can be different. It promotes interoperability in terms of technical interoperability or common standards; work on establishing comparable protection from legal frameworks or recognition of legal and regulatory effects (either autonomously or through mutual recognition); shared support for the establishment of broader international frameworks; and the exchange knowledge and best practices on policies, regulation, technical, security standards and user adoption of digital identities.

DEPA as a building block

DEPA was designed as a building block for other agreements. The New Zealand Ministry of Foreign Affairs and Trade website notes that those involved "hope that this new agreement will generate new ideas and approaches that can be used by members in the WTO negotiations, and by other countries negotiating free trade agreements or engaging in international digital economy or digital trade work."[31] The modular nature of the text means that individual elements can easily be plucked out and inserted into others'

29 DEA, Art. 10, 11, 29-32.

30 DEPA, Module 7; for New Zealand's approach, see https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-trust-framework/; for Singapore's approach, see https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi

31 New Zealand Ministry of Foreign Affairs and Trade (https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement/overview/).

agreements or used as a model in the WTO process. DEPA is also open to all who can meet its high standards, and indeed Canada has recently signalled an interest in joining the agreement.[32]

Whether through broadening participation or through the uptake of modules of the text in other settings, DEPA helps to streamline the 'digital noodle bowl'. In fact, the significance of the agreement is less about the economic integration of the countries concerned than it is about the demonstration effect to larger players in the global system.

In fact, the DEPA is an example of New Zealand's trade strategy of "open concerted plurilateralism" – working with likeminded partners to develop innovative new trade policy models that can eventually expand and build towards broader multilateral outcomes.[33] This is a salient difference to DEA, which is a 'closed' model (being part of a bilateral FTA). While in some areas, DEA has been able to go further into the granular detail than DEPA – for example, mapping out with a far greater level of specificity the bilateral work that is need to create interoperable digital identities in the relevant MoU – the fact that it is not open to others to join mean that it has less potential as a building block to broader outcomes, although it is certainly not a stumbling block either.

In an ideal world, these two agreements would be brought together, with Australia acceding to DEPA and both Australia and Singapore seeking to bring their experiences with more detailed bilateral cooperation in DEA to bear on the DEPA work programme.

A PERFECT EXCUSE FOR A CONVERSATION: DIGITAL IN APEC

Complementing the Asia-Pacific FTA policymaking discussed above, there is also active work on digital trade topics in the APEC context. That work can potentially play a valuable supporting role in understanding impediments to digital trade in the region and developing strategies to minimise them, in a process that involves not just like-minded economies (as for DEPA or DEA), but also some that take a very different view on issues such as data flows – including the United States, China, Russia and others (APEC Policy Support Unit 2019).

APEC has an ambitious agenda for the digital economy, set out in the 2017 APEC Internet and Digital Economy Roadmap. As is the case for DEPA and DEA, the Roadmap takes a broad view on what is needed to address the impediments to digital trade, stating that "[i]t is because of its very pervasiveness that *holistically* understanding the impact and *coordinating* the benefits deriving from the Internet and Digital Economy has become so important" (APEC 2017). It includes sections on the development of digital infrastructure and universal access to broadband, the promotion of interoperability, cooperation and

32 DEPA Module 16 (see also https://www.beehive.govt.nz/release/canadian-interest-digital-economy-partnership-agreement-welcomed).
33 See, for example, the speech by the then New Zealand Minister of Trade and Export Growth on 23 July 2020 at https://www.beehive.govt.nz/speech/trade-all-and-state-international-trade.

coherence in regulatory approaches, the development of holistic policy frameworks (including bringing in sectors such as agriculture), promoting innovation, enhancing trust and security, data flows, measurement, inclusion and e-commerce.[34]

By deliberate design, APEC is collaborative, voluntary, and non-binding. This means that it has a reputation as an 'incubator of ideas' in policymaking. Indeed, it can be argued that the full realisation of the 'hard rules' of CPTPP, RCEP and even DEPA and DEA has taken place against the backdrop of patient work in APEC to build confidence through the development of soft norms which eventually found their way into those trade agreements. While concrete outcomes from the Roadmap have been limited to date, this year APEC is mapping out a work programme for the next two decades, including on the digital economy and innovation. There is significant potential for APEC economies to build on DEPA and DEA to develop more coherent approaches in APEC-wide policy discussions, and in turn champion some of those concepts in other settings.

CONCLUSION: GLOBAL RULES WOULD BE FIRST-BEST

The first-best outcome for businesses would unquestionably be to establish *global* rules that would mitigate and minimise impediments to digital trade, including seeking to untangle the digital noodle bowl across as many markets as possible. The WTO would seem to be the obvious forum for this. A group of nearly 90 WTO members, accounting for more than 90% of global trade and representing all major geographical regions and levels of development, is currently engaged in negotiations on "e-commerce" (UNCTAD 2021). Recent reports suggest that, while some good progress has been made on some elements (including those with practical commercial value in the short term, such as digital trade facilitation and spam), the negotiations are not yet at the point of "achieving WTO-plus outcomes that deliver meaningful benefits for businesses and consumers" as is their goal. [35] Wide gaps remain on the most contentious issues including data flows; emerging technologies and some of the other elements in DEPA and DEA are not even on the agenda.

All bar one of the 21 APEC member economies are participants in the WTO plurilateral negotiations on e-commerce (UNCTAD 2021). Drawing on their experiences in the development of both hard trade rules and soft norms for the digital economy, Asia-Pacific digital trade policy innovators can potentially play an important role in that WTO negotiation in helping to shape global thinking about how to address current digital trade barriers, as well as how to develop more creative approaches that favour agile, flexible, interoperable and business-friendly digital trade policy to unlock the full potential of the digital economy.

34 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group

35 'WTO Joint Statement Initiative of E-Commerce: Co-Convenors' Update Released', Japanese Ministry of Economy, Trade and Industry, 15 December 2020 (https://www.meti.go.jp/english/press/2020/1215_001.html).

REFERENCES

Aaronson, S (2019), "What Are We Talking about When We Talk about Digital Protectionism?", *World Trade Review* 18(4): 541-577.

Aaronson, S and P Leblond (2018), "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO", *Journal of International Economic Law* 21: 245-272.

ABAC – APEC Business Advisory Council (2015) *Driving Economic Growth through Cross-Border E-Commerce in APEC: Empowering MSMEs and Eliminating Barriers*, USC Marshall School of Business.

ABAC (2018) *Realising the Untapped Potential of MSMEs in APEC: Practical Recommendations for Enhancing Cross-Border Trade*, USC Marshall School of Business.

ABAC (2019), *Bridging the Digital Divide: Navigating Cross-Border Non-Tariff Barriers,* USC Marshall School of Business.

APEC (2017), "APEC Internet and Digital Economy Roadmap", 2017/CSOM/006.

APEC Policy Support Unit (2019), "Fostering an Enabling Policy and Regulatory Environment for Data-Utilizing Businesses", July 2019.

Baldwin, R (2016), *The Great Convergence*, Harvard University Press.

Baldwin, R (2019), *The Globotics Upheaval*, Harvard University Press.

Bhagwati, J (1995), "US Trade Policy: The Infatuation with FTAs", Columbia University Discussion Paper Series 726.

Bughin J, J Seong, J Manyika, M Chui and R Joshi (2018), *Notes from the AI Frontier: Modeling the Impact of AI on the World Economy*, McKinsey Global Institute.

Burri, M (2020), "Data Flows and Global Trade Law: Tracing Developments in Preferential Trade Agreements", forthcoming in M Burri (ed), *Big Data and Global Trade Law,* Cambridge University Press (forthcoming).

Burri M and R Polanco (2020), "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset", *Journal of International Economic Law* 23(1): 1-34.

Ferracane, M (2017), "Restrictions on Cross-Border Data Flows: A Taxonomy", ECIPE Working Paper No.1/2017.

Hootsuite and We Are Social (2021), *The Global State of Digital 2021* (https://www.hootsuite.com/resources/digital-trends).

IMF (2021), "World Economic Outlook Update: Policy Support and Vaccines Expected to Lift Activity", January.

Kawai, M and G Wignaraja (2009), "The Asian 'Noodle Bowl': Is It Serious for Business?", ADBI Working Paper 136, Asian Development Bank Institute.

López González, J and J Ferencz (2018), "Digital Trade and Market Openness", OECD Trade Policy Papers No. 2017.

Lund, S, J Manyika, J Woetzel, J Bughin, M Krishnan, J Seong and M Muir (2019), *Globalization in Transition: The Future of Trade and Value Chains*, McKinsey Global Institute.

Manyika, J, S Lund, J Bughin, J Woetzel, K Stamenov and D Dhingra (2016), *Digital Globalisation: The New Era of Digital Flows*, McKinsey Global Institute.

Meltzer J (2019), "Governing Digital Trade", *World Trade Review* 18(S1): s23-s48

Meltzer J and P Lovelock (2018), "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia", Brookings Working Paper No. 113.

OECD (2020), "Leveraging Digital Trade to Fight the Consequences of COVID-19", OECD Brief, 7 July.

TRPC (2020), "Australia-Singapore Digital Economy Cooperation on Standards", September.

UNCTAD – United Nations Conference on Trade and Development (2021), "What is at Stake for Developing Countries in Trade Negotiations on E-Commerce? The Case of the Joint Statement Initiative".

United Nations (2017), *Digitalization, Trade and Development*, UNCTAD Information Economy Report 2017.

van der Marel, E (2020), "Lessons from the pandemic for trade cooperation in digital services", in S J Evenett and R Baldwin (eds), *Revitalising Multilateralism: Pragmatic Ideas for the New WTO Director-General*, CEPR Press.

van der Marel, E, H Lee-Makiyama, M Bauer and B Verschelde (2014), "The Costs of Data Localisation: A Friendly Fire on Economic Recovery", ECIPE Occasional Paper No. 3/2014.

WTO (2021), "Services trade recovery not yet in sight", 26 January (www.wto.org/english/news_e/news21_e/serv_26jan21_e.htm).

Wu, M (2017), "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System", RTA Exchange, ICTSD and IDB, November.

ABOUT THE AUTHOR

Stephanie Honey is the Director of Honey Consulting Ltd. She is a former New Zealand trade negotiator and currently also serves as the Deputy Executive Director of the APEC Business Advisory Council and Associate Director of the New Zealand International Business Forum.

CEPR PRESS

UKTPO UK TRADE POLICY OBSERVATORY | US UNIVERSITY OF SUSSEX

Digital trade and digitally enabled services hold the promise of much-needed future growth and prosperity. Yet digital trade is different: it is intrinsically linked to cross-border data flows, it often relies on digital platforms as intermediaries, and it is driven by rapidly advancing technologies such as artificial intelligence. For all its opportunities, these features pose unique challenges for trade policymaking.

Thus in March 2021, the UK Department for Digital, Culture, Media and Sport and the UK Trade Policy Observatory organised a conference, hosted by CEPR, to discuss new directions for digital trade policy. This eBook presents the conference proceedings. Part 1 sets out to identify impediments to digital trade, generally and in specific contexts, whereas Part 2 discusses policy options to address them. Contributions in the first part include proposals to collect information and map policy stances towards digital trade and cross-border data flows, a comparison of source code disclosure requirements in free trade agreements, and a discussion of IP-related issues that arise at the intersection of artificial intelligence and international trade. The second part discusses various aspects of data governance as a facilitator of digital trade, from the role of copyright and trade secret law to the idea of a single data area overseen by an International Data Standards Board. One chapter describes the forefront of digital trade policymaking that is currently developing in the Asia-Pacific region.

Looking ahead, new forms of digital protectionism may arise. Potential barriers to digital trade may encompass polices to limit disinformation, regulations on algorithmic decision-making, censorship, internet shutdowns or cybersecurity rules. Innovative solutions will need to be found to safeguard the trusted environment for data flows that is vital for digital trade to flourish.

ISBN: 978-1-912179-42-8

ISBN 978-1-912179-42-8
9 781912 179428

UK Trade Policy Observatory
University of Sussex | Jubilee Building | Falmer | BN1 9SL

Centre for Economic Policy Research
33 Great Sutton Street | LONDON EC1V 0DX | UK
TEL: +44 (0)20 7183 8801 | FAX: +44 (0)20 7183 8820
EMAIL: CEPR@CEPR.ORG
WWW.CEPR.ORG