BSG Working Paper Series

Providing access to the latest policy-relevant research

The UK and digital trade: Which way forward?

BSG-WP-2021/038

February 2021

DOI: https://doi.org/10.35489/BSG-WP-2021/038

Emily Jones, Blavatnik School of Government, University of Oxford

Beatriz Kira, Digital Pathways, Blavatnik School of Government, University of Oxford

Danilo B. Garrido Alves, Global Economic Governance, Blavatnik School of Government, University of Oxford

Anna Sands, Global Economic Governance, Blavatnik School of Government, University of Oxford

The UK and digital trade: Which way forward?

BSG-WP-2021/038
February 2021
DOI: https://doi.org/10.35489/BSG-WP-2021/038

Emily Jones, Associate Professor in Public Policy, Blavatnik School of Government, University of Oxford
Beatriz Kira, Senior Research and Policy Officer, Digital Pathways, Blavatnik School of Government, University of Oxford
Danilo B. Garrido Alves, Research Officer, Global Economic Governance, Blavatnik School of Government, University of Oxford
Anna Sands, Research Officer, Global Economic Governance, Blavatnik School of Government, University of Oxford

Abstract

The internet and digital technologies are upending global trade. Industries and supply chains are being transformed, and the movement of data across borders is now central to the operation of the global economy. Provisions in trade agreements address many aspects of the digital economy – from cross-border data flows, to the protection of citizens' personal data, and the regulation of the internet and new technologies like artificial intelligence and algorithmic decision-making.

The UK Government has identified digital trade as a priority in its Global Britain strategy and one of the main sources of economic growth to recover from the pandemic. It wants the UK to play a leading role in setting the international standards and regulations that govern the global digital economy. The regulation of digital trade is a fast-evolving and contentious issue, and the US, European Union (EU), and China have adopted different approaches. Now that the UK has left the EU, it will need to navigate across multiple and often conflicting digital realms. The UK needs to decide which policy objectives it will prioritise, how to regulate the digital economy domestically, and how best to achieve its priorities when negotiating international trade agreements. There is an urgent need to develop a robust, evidence-based approach to the UK's digital trade strategy that takes into account the perspectives of businesses, workers, and citizens, as well as the approaches of other countries in the global economy.

This working paper aims to inform UK policy debates by assessing the state of play in digital trade globally. We present a detailed analysis of five policy areas that are central to discussions on digital trade for the UK: cross-border data flows and privacy; internet access and content regulation; intellectual property and innovation; e-commerce (including trade facilitation and consumer protection); and taxation (customs duties on e-commerce and digital services taxes). In each of these areas we compare and contrast the approaches taken by the US, EU and China, discuss the public policy implications, and examine the choices facing the UK.

Acknowledgments

This publication arises from activities funded by Research England's Strategic Priorities Fund allocation to the University of Oxford.

For helpful feedback and insightful comments, we would like to thank participants of one academic workshop hosted virtually by the Blavatik School of Government in November 2020 and one multi-stakeholder workshop jointly organised by the Blavatik School of Government, the International Chamber of Commerce, and the Open Rights Groups in January 2021. We are particularly grateful to Elizabeth Stuart, Eleonor Duhs, Anna Fields, Javier Ruiz, Joshua Meltzer, Kristina Irion, Svetlana Yakovleva, Sandra Wachter, Vicki Nash, Ingo Borchert, Jason Stockwood, and Simon Roberts for comments to earlier versions of this paper and for conversations that helped us to sharpen our arguments. We thank Kirsten Hunter and Beth Keehn for copyediting the paper. All errors remain our own.

Table of contents

List of acronyms **3**
1 Introduction **4**
2 Bringing trade agreements in line with the digital economy **5**
3 Competing approaches to digital trade: US, EU and China **8**
US approach 8
EU approach 9
China's approach 11
Other countries – navigating between competing regulatory spheres ... 12
4 Policy issues in detail **13**
4.1 Cross-border data flows, data localisation and personal data protection **13**
Overview of policy issues 14
US approach in trade agreements 16
EU approach in trade agreements 18
China's approach in trade agreements 21
DEPA 22
UK approach in trade agreements 23
4.2 Internet access and content regulation **25**
Overview of policy issues 25
US approach in trade agreements 26
EU approach in trade agreements 28
China's approach in trade agreements 29
DEPA 30
UK approach in trade agreements 31
4.3 Intellectual property (IP) protection and innovation **33**
Overview of policy issues 33
US approach in trade agreements 36
EU approach in trade agreements 36
China's approach in trade agreements 37
DEPA 37
Japan's approach in trade agreements 38
UK approach in trade agreements 38
4.4 E-commerce – trade facilitation and consumer protection **39**
Overview of policy issues 39
US approach in trade agreements 41

EU approach in trade agreements 42
China's approach in trade agreements 42
DEPA 44
UK approach in trade agreements 45
4.5 Customs duties and digital services taxes 46
Overview of policy issues 46
US approach in trade agreements 48
EU approach in trade agreements 49
China's approach in trade agreements 50
DEPA 50
UK approach in trade agreements 50
5. Conclusion 51

List of acronyms

AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
CDA	Communications Decency Act
CEPA	UK-Japan Comprehensive Economic Partnership Agreement
CETA	EU-Canada Agreement
CJEU	Court of Justice of the European Union
COPPA	Children's Online Privacy Protection Act
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DMCA	Digital Millennium Copyright Act
DEPA	Digital Economy Partnership Agreement
DPA	Data Protection Authority
DSA	Digital Services Act
DST	Digital Services Tax
EPA	Economic Partnership Agreement
FCC	Federal Communications Commission
FTA	Free Trade Agreement
FTC	Federal Trade Commission
GATS	General Agreement on Trade in Services
GDPR	General Data Protection Regulation
GLBA	Gramm Leach Bliley Act
IP	Intellectual Property
ISP	Internet Service Provider
OECD	Organisation for Economic Co-operation and Development
OHWP	Online Harms White Paper
OSP	Online Service Providers
PIPEDA	Personal Information Protection and Electronic Documents Act
RCEP	Regional Comprehensive Economic Partnership
SCC	Standard Contractual Clauses
TCA	Trade and Cooperation Agreement Between the EU and the UK
TiSA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
UGC	User-generated content
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
URL	uniform research locator
USMCA	United States-Mexico-Canada Agreement
USTR	Office of the United States Trade Representative
WTO	World Trade Organization

1 Introduction

Digital trade is a strategic priority for the UK Government. The UK's digital sector is sizeable and growing rapidly. It accounted for an estimated 7.6% of the UK economy in 2019, employed an estimated 1.7 million people in 2020, and is growing more rapidly than most other sectors.[1] UK trade flows are increasingly digital: an estimated two-thirds of UK services exports and a half of UK services imports were digitally delivered in 2018.[2] The government has identified the growth and development of the UK's digital economy as a strategic priority in its Global Britain economic agenda, and is aiming for the UK to be a leading voice in digital trade, shaping the global governance of the digital economy.[3]

On the global stage, the regulation of digital trade is a fast-evolving and contentious issue. The UK faces important decisions about how to regulate the digital economy now that it has left the EU, including identifying which policy objectives will be prioritised, the optimal regulatory measures for furthering these objectives, and how best to achieve them when negotiating international trade agreements. Provisions in trade agreements address many aspects of the digital economy – from cross-border data flows, to the protection of citizens' personal data, and the regulation of the internet and new technologies like artificial intelligence (AI) and algorithmic decision-making. Policy decisions have implications for large and small businesses, consumers, and workers.

There is no consensus internationally on how best to regulate the digital economy, and the UK will need to chart a course forward that takes into account the very different approaches of the US, EU, and China – the three digital superpowers in the world economy. For instance, the EU places greater priority on data privacy and consumer protection in its international trade agreements than the US, which prioritises ensuring the free flow of data across borders and protecting the intellectual property (IP) of its businesses. While the UK has been aligned with the EU's approach, the recent UK–Japan agreement signals that the UK is moving towards the approach taken by the US and many Asia-Pacific countries in their recent trade agreements.[4]

During 2021, the UK will be negotiating digital trade provisions as it negotiates in free trade agreements, including with Australia, New Zealand, Canada, and the US; as it looks to accede to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Even with the recently agreed EU–UK Trade and Cooperation Agreement (TCA), there are still outstanding points related to digital trade to be agreed in the coming months. Importantly, as discussed below, the European Commission will decide whether to grant the UK an adequacy decision allowing the free flow of data from the EU to the UK to continue.[5] While digital trade is a priority for the UK Government, it is yet to set out a strategy. This working paper takes stock of how other countries approach digital trade, the public policy implications of different policy approaches, and the choices facing the UK.

Section 2 of this paper explains what digital trade is and where international negotiations on digital trade are taking place. Section 3 gives an overview of the different regulatory approaches of the US, EU, and China. Section 4 is the heart of

the paper and it presents detailed analysis of five different areas of digital trade. In each of these areas we compare and contrast the approaches taken by the US, EU and China, discuss the associated public policy implications, and examine the choices facing the UK. The five areas are: cross-border data flows; internet access and content regulation; IP and innovation; e-commerce (including trade facilitation); and customs duties and digital services tax. The paper concludes in Section 5 by highlighting emerging issues in digital trade, including discussions over cybersecurity, and emphasising the need for a robust, evidence-based approach to digital trade policy that takes into account the perspectives of a wide range of UK stakeholders.

2 Bringing trade agreements in line with the digital economy

The rapid developments of technologies such as AI, robotics, autonomous vehicles, 3D printing, and nanotechnology have triggered a new wave of economic structural change, often termed the 'Fourth Industrial Revolution'.[6] Digital technologies, products and services have become core aspects of almost every sector, impacting on production processes and business models, disrupting established sectors and altering the dynamics of the world economy.[7]

Digitalisation is affecting trade in many different ways. The services sector is arguably most impacted by digitalisation, and there has been a surge in digitally delivered services such as the streaming of movies, internet banking, and professional services such as accounting. Digitalisation improves traditional supply chains, including by making logistics more efficient, and firms increasingly communicate with suppliers and customers and raise funds online.[8] As a result of digitalisation, trade in smaller, often lower-value physical goods (parcels ordered online) are growing, and new types of bundled goods and services are emerging (such as autonomous cars).

The movement of data, or information, across borders underpins these processes of digitalisation.[9] The digital economy arose out of the extraordinary amounts of detailed machine-readable information that have become available about practically all personal, social and business activities and interactions. Data is at the core of new and rapidly growing service supply models such as cloud computing, the Internet of Things, and additive manufacturing. It also underpins trade by enabling the co-ordination of global value chains and enabling the implementation of more efficient trade facilitation.[10]

In this fast-evolving environment, governments are facing growing regulatory challenges, not just in managing issues arising from digital disruption, but also in ensuring that the opportunities and benefits from the global digital economy can be realised and shared inclusively. In the area of data flows, for instance, governments need to find ways to achieve public policy objectives such as privacy or security, and ensure cybersecurity, while maintaining the benefits of the cross-border data flows that underpin the digital economy. In the area of IP, governments are tasked with protecting the IP of digital economy firms while also ensuring effective oversight and accountability of new technologies. The digital economy also raises questions about how the internet should be regulated in order to protect internet users and

prevent harms (ranging from hate speech to non-consensual pornography), promote fundamental rights such as free expression and information access, and encourage economic growth and technical innovation.

In a hyper-connected global economy, the policies and regulations adopted in one jurisdiction have implications for others, creating both positive and negative spill-overs.[11] Governments have increasingly turned to trade agreements to set new rules to govern the digital economy. When World Trade Organization (WTO) members started to discuss digital trade in the late 1990s, the focus was on the digitalisation of supply chains and negotiations addressed e-commerce – the production, distribution, marketing, sale or delivery of goods and services by electronic means.[12] Since then the scope of discussions has widened to include many other issues central to the governance of the digital economy, including cross-border data flows, the regulation of new digital technologies and of the internet. In the words of Valente, digital trade negotiations encompass "far more than Amazon, MercadoLibre, Alibaba and eBay: they are about a broader digital economy that includes the so-called 'sharing economy', the trade in digital goods such as e-books and digital music, and hybrid areas such as digital design of physical products, web platforms, and AI applications".[13]

As the impacts of digitalisation on trade are so widespread and the nature of policy discussions over digital trade have evolved over time, there is no settled definition of digital trade. In a bid to start measuring digital trade flows, the OECD has settled on a definition of digital trade as "all trade that is digitally ordered and/or digitally delivered".[14] In this paper, our focus is on the key policy areas covered in the e-commerce and digital trade chapters of recent trade agreements.

Against the background of the rapid and far-reaching changes brought by digitalisation, it is often said that the rules that underpin the digital trade environment have struggled to keep pace with changing business models. Existing multilateral trade rules were negotiated when digital trade was in its infancy but nonetheless have implications for digital trade as they are technologically neutral (so apply irrespective of the technology through which the good or service is delivered). For instance, the WTO's General Agreement on Trade in Services (GATS) aims at liberalising services sectors and harmonising regulatory approaches, and has implications for services that are digitally provided. In addition to covering digitally provided services such as accounting, the 'technological neutrality' of GATS allows it to address 'digital products' such as e-books and downloadable movies and music. Similarly, the WTO's Technical Barriers to Trade (TBT) Agreement aims to ensure that technical standards regulating safety, quality and other characteristics of products are non-discriminatory and do not create unnecessary obstacles to trade, and applies to the use of technical standards for information and telecommunications and electronic products (such as standards governing broadband networks or regulations on encryption). Meanwhile, the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) covers IP rights protection for technologies that enable e-commerce, such as computers, software, routers, networks, switches, and user interfaces. In addition, e-commerce

transactions can involve digital products with copyright-protected content that contributes to its value, such as e-books.[15]

Because the existing WTO rules were negotiated before the digital economy took off, there are major uncertainties about how they should be applied. For instance, under GATS, governments have scheduled specific sectors for liberalisation, and have committed not to introduce restrictions to the cross-border flow of services in these sectors, subject to some exceptions. Interpreting these commitments for the digital era requires classifying the sector in which digital products fall, and this is far from trivial. For instance, if online platforms and the services they offer were classified as computer services, most governments would have to grant full access to foreign services and services suppliers and treat them as they treat domestic ones – because of the high level of existing commitments under the GATS of virtually all WTO Members. On the other hand, if online games were classified as audiovisual services, most WTO Members would have the policy space to maintain and adopt restrictive and discriminatory measures.[16] Another challenge is that traditional WTO rules treat goods and services differently, but an increasing number of 'smart' products combine these features. Moreover, existing multilateral trade rules do not cover areas such as cross-border data flows, which are central to the global digital economy.

There have been various attempts to update WTO rules to bring them in line with the realities of the digital economy. However, negotiations at the WTO stalled at the end of the 1990s – the so-called Doha Development Round of negotiations – due to major tensions between industrialised and developing countries. As multilateral negotiations stalled, WTO Members turned to plurilateral negotiations (negotiated among sub-groups of WTO Members). In 2013, a group of 23 WTO Members started negotiating a plurilateral Trade in Services Agreement (TiSA), led by the US and Australia, the EU and a group of 'like-minded' countries, but these also stalled.[17] Since 2019, a sub-group of WTO Members (currently 86 countries) have been negotiating a 'Joint Statement Initiative on e-commerce'.[18] The group is co-convened by Australia, Japan, and Singapore, and has a broader membership including the US, EU, and China (although India and South Africa have not joined). As at January 2021, Members were negotiating text proposals in a range of areas, including data flows, unsolicited electronic messages (spam), source code, open government data, trade facilitation in goods, services market access, electronic signatures (e-signatures) and authentication, and online consumer protection.[19]

As WTO talks have made limited progress, governments have turned to bilateral and regional trade agreements where provisions on e-commerce, and later wider aspects of digital trade, have been included since the early 2000s. As at October 2018, two-thirds of WTO Members (113 of 164) were party to bilateral and regional trade agreements with provisions on digital trade.[20] These agreements vary substantially in scope and depth. The US has championed the inclusion of digital trade provisions in trade agreements, and its agreements with several countries (including Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries, Panama, Colombia and South Korea) all contain commitments that go beyond the WTO in the sense of being more stringent and addressing issues

not covered by the WTO. In addition to governing digital trade with specific trading partners, the US looks to use its bilateral and regional agreements to set a precedent for global negotiations on digital trade.

The emergent regulatory template on digital issues is not limited to US agreements. Singapore, Australia, Japan, and Colombia have been among the major drivers of trade agreements with more extensive digital trade provisions, although the issues covered and the levels of legalisation still vary substantially. Although the EU has digital trade provisions in many of its trade agreements, it is only in the very recent agreements that there is a dedicated chapter on digital trade and some substantive provisions: beforehand there were only a few provisions, usually as part of services chapters, and they were limited to upholding WTO commitments and pledges of co-operation.[21] China is similar, in that its trade agreements have only recently started to contain substantive provisions on digital trade.

While this paper focuses on provisions in trade agreements, they are not the only forum where new rules and regulations for the global digital economy are being negotiated. Under the auspices of international standard-setting bodies including the International Electrotechnical Commission (IEC), International Organization for Standardization (ISO), and International Telecommunication Union (ITU), governments negotiated new standards for regulating the digital economy. While couched in dry, technical language, these standards regulate digital technologies and are key to enabling global supply chains and facilitating global trade. They provide a harmonised, stable and globally recognised framework for the dissemination and use of technologies.[22] As with other aspects of the digital economy, negotiations over these standards have political dimensions, and while the US has turned to trade agreements to promote its digital economy interests, the Chinese Government has sought to influence these standard-setting processes.[23] Similarly, the EU looks outside of trade agreements to promote global convergence on high standards of data protection, by encouraging countries to accede to the Council of Europe Convention 108 (the only legally binding multilateral instrument on data protection, with signatories committing to uphold similar levels of protection to the GDPR).[24]

3 Competing approaches to digital trade: US, EU and China

The US, EU, and China are the three most influential players in the global digital economy. They take very different approaches in how they regulate the digital economy and to the provisions they negotiate on digital trade in trade agreements. As the UK develops its own digital trade strategy, it is vital to understand how these three jurisdictions approach digital trade. This section gives an overview of the approaches taken by the US, EU, and China and their policy priorities. The subsequent section examines specific issues in depth.

US approach

The US is home to most of the world's largest internet companies and digital service suppliers and its lax regulatory environment allowed technology companies to grow

at exponential speed. One US company alone provides almost one half of the worldwide cloud-computing capacity.[25] Four of the top five internet companies in the world are based in the US: Amazon, Alphabet (Google), Facebook, and Microsoft.[26] These companies are mostly service providers that offer online search, social network or content services, but many of them also provide the hardware, software, and platforms for digital trade. For these companies it is crucial to have free flow of information across the globe and autonomy in deciding where to locate their computing facilities and servers.

The focus of the US government in trade negotiations has been to secure increased market access and IP protection for these large technology companies, including by securing commitments from other governments that they will not impede cross-border flows of data or require private companies to disclose source code or algorithms, except in a very narrow range of circumstances. Securing ambitious provisions on digital trade was a strategic priority in the Trans-Pacific Partnership (TPP), negotiated under the Obama administration. Although President Trump withdrew the US from the TPP, the digital trade provisions were incorporated into the new CPTPP that the remaining 11 TPP Members signed in 2018. The Trump administration continued to build from the TPP, and similar provisions are found in the US–Mexico–Canada Agreement (USMCA) and in the US–Japan Digital Trade Agreement, and are reflected in recent US proposals at the WTO.[27]

Under the Trump administration, greater attention was been paid to protecting US national security interests and the domestic market. In 2019 the US government introduced an executive order that gave the federal government the power to prevent US companies from buying foreign-made telecommunications equipment (deemed a national security risk), which was used to block Chinese companies like Huawei from doing business in the US. The US government also sought to ban the activities of the popular Chinese apps WeChat and TikTok on national security grounds, with concerns raised that the data they collected from US households could be used for espionage (although these moves were halted by US courts).[28] With the rise of security tensions and growing economic rivalry between the US and China, there are concerns that the digital economy is Balkanising, divided into different digital realms.

There are also major policy debates in the US over whether (and to what extent) internet companies should have liability for online content, and for data privacy. There are proposals to introduce federal privacy legislation and alter legislation on the liability of internet companies, and a series of antitrust cases are being pursued against the largest technology companies due to concerns over anti-competitive behaviour. As US policy priorities shifts, this is likely to impact its approach in trade negotiations, as we discuss in more detail below.

EU approach

In contrast with the US, the EU has few large technology companies, accounting for only 4% of the market capitalisation value of the world's 70 largest digital platforms.[29] However, the EU is a large market for digital products and its policy priority has been

to promote its citizens' consumer and digital rights. This has been most pronounced in the area of data privacy, where the EU introduced a stringent privacy regime for personal data, the General Data Protection Regulation (GDPR). The EU has been at the forefront of initiatives to curb anti-competitive practices of large internet companies, and EU Member states have been leading the charge on the introduction of digital services taxes.

Rather than turn to trade agreements, the EU has relied foremost on leveraging its market power to ensure that other governments uphold the digital rights of EU citizens – the 'Brussels effect'.[30] The EU only allows its citizens' data to be transferred to other jurisdictions when it deems that other governments provide a sufficient level of data protection. Many countries have based their approach to data privacy on the GDPR, with the EU officially recognising 12 jurisdictions as having equivalent standards to its own (so-called 'adequacy decisions'), thereby allowing the data of EU citizens to flow freely to these jurisdictions.[31] In the absence of a federal law on data privacy in the US, some individual states, including California, are moving to adopt legislation similar to the GDPR.

Although the GDPR is increasingly seen as the global standard for data protection, tensions persist, particularly between the US and EU. The US government and large US companies lobbied strongly against the EU's adoption of the GDPR, and the US continues to argue that it creates disproportionate barriers to trade.[32] After the GDPR was implemented by the EU, many large US companies complied in order do business in the EU, despite the high costs: as at May 2018, US Fortune 500 companies had spent approximately US$7.8 billion on GDPR compliance, averaging US$16 million per company.[33] Although individual companies and some US states have aligned their data protection practices with the EU, at a federal level, the US approach remains much weaker. In July 2020, Court of Justice of the European Union (CJEU) struck down the US–EU agreement on data flows – the so-called 'Privacy Shield' – for failing to sufficiently protect EU citizens' right to privacy.

In its trade agreements, the EU has, until recently, taken a minimalist approach, seeking to preserve a high level of regulatory autonomy. The EU has committed to prohibitions on customs duties on e-commerce, the promotion of e-authentication and e-signatures, and, more recently, bans on data localisation. Alongside these moves to promote digital trade, the EU has also promoted the inclusion of stand-alone articles on the 'right to regulate' and on data privacy.[34]

Provisions on data flows have posed challenges, as the EU has struggled to find a formulation for legal provisions that would both cross-border data flows and simultaneously uphold citizens' right to privacy, which is considered a fundamental human right in the EU.[35] Following lengthy internal discussions, in 2018 the European Council agreed that commitments could be made on cross-border data flows in trade agreements so long as privacy was recognised as a fundamental, non-negotiable right and broad exceptions were included that preserve full regulatory autonomy with regards to the right to privacy.[36] The EU–UK agreement, for instance, includes a stand-alone article on privacy that stipulates "Nothing in this Agreement

shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy" (art. DIGIT.7 TCA).

As with the GDPR, the EU's approach to digital trade provisions in trade agreements has been criticised by the US government, large technology companies, and some think tanks as being unduly protectionist. Although digital trade flows between the US and EU are the most extensive in the world, stark differences over digital trade were a major impediment to the conclusion of the Transatlantic Trade and Investment Partnership (TTIP) between the EU and US. There are also tensions between the EU and China, with the EU opposing technology transfer requirements and raising national security concerns over the use of Chinese technology in critical infrastructure. However, the EU has opted for a more diplomacy-based approach than the US, entering into a high-level dialogue with the Chinese government, concluding an EU–China investment agreement at the end of 2020, with some provisions on the digital economy, including prohibitions on technology transfer requirements.[37]

In 2020, the EU announced a shift towards technology sovereignty and proposed more stringent regulation of emerging technologies, such as including mandatory 'conformity assessment' tests for AI before they can be marketed in the EU, and regulatory initiatives to ensure consumer security and safety. Discussion is underway on proposals to enhance the EU's data sovereignty, including data residency and localisation requirements in the context of a new 'European cloud'.[38] The European Commission has also announced two new major regulations – the Digital Services Act (DSA) and the Digital Markets Act (DMA) – which set out a common set of rules for intermediary liability and a specific regulatory approach for systemically important 'gatekeeper' companies.[39] It is unclear exactly what this implies for the European future approach in trade agreements, although it does suggest that the EU will be wary of any provisions that constrain its regulatory autonomy. This sets it fundamentally against many aspects of the US approach to date.

China's approach

Over the past 20 years, China has taken a protectionist approach to the digital economy in order to support its own industry. Until very recently, it has also been wary of including binding commitments on digital trade in its free trade agreements. The Chinese government has used two main types of regulations:

- The first regulates the hardware or the facilities. Under the Provisional Regulations on the Management of International Networking of Computer Information Networks (1996), connection to international networks must go through international gateway provided by the Ministry of Posts and Telecommunications. Firms and individuals are prohibited from establishing or using any other gateways, and all new internet networks must be approved by the State Council.
- The second focuses on the content. The Regulation on Internet Information Service (2000) prohibits a wide range of content, such as information endangering national security, leaking state secrets, harming state honour

and interests, spreading rumours, disrupting social order and stability. Unlike the US, internet information service providers are not exonerated from liabilities arising from user-generated contents, as further discussed in section 4.2.[40]

The large, protected Chinese market worked to the advantage of domestic companies, even though it constrained them from becoming global players. Foreign companies wishing to enter the Chinese market have been subject to the same restrictions as Chinese companies and they have found it particularly hard to adjust their business models to fit the restrictive regulatory environment in China. Internet restrictions helped to shield Chinese firms like Baidu and Tencent from competition from international firms like Google and Facebook. Due in part to the sheer size of the Chinese domestic market, they became some of the largest internet companies in the world.[41] China is home to three of the 10 largest internet companies in the world (Alibaba, Tencent, Baidu).[42] While the largest US internet companies mainly provide online search, social network or content services, two of the top Chinese companies mainly sell physical goods online.

While the Chinese government has been wary of including commitments on digital trade in its trade agreements, this has started to shift as the largest Chinese companies have sought to expand internationally. From 2015, China started including digital trade provisions in trade agreements. It is now taking part in discussions on e-commerce at the WTO and is playing an active role in influencing international standards for new digital economy products.[43] Reflecting the interests of its largest internet companies, China's strategic priority has been to facilitate traditional trade in goods enabled by the internet.[44] Thus, while China continues to oppose binding rules on data flows or language that limits digital protectionism, it has included provisions that encourage e-commerce in recent agreements with Korea, Australia, and Chile.[45] China is a signatory to the Regional Comprehensive Economic Partnership (RCEP) agreement (2020), which includes the Association of Southeast Asian Nations (ASEAN), Australia, India, Japan, South Korea, and New Zealand. The e-commerce section (4.4 below) includes provisions on cross-border data flows, data localisation, and disclosure of source code, but these are non-enforceable and subject to wide-ranging exceptions.[46]

In China, like the US and EU, the government is reviewing how it regulates large digital companies. In November 2020, the government introduced new antitrust guidelines, signalling a shift from allowing the rapid growth and market dominance of a few large companies to an approach that seeks to promote greater competition.[47] It is unclear how this will affect China's approach to digital trade, and major tensions remain between the US, EU, and China.

Other countries – navigating between competing regulatory spheres

Strategic rivalry between the US, China, and (to some extent) the EU is generating concerns over the Balkanisation of the digital economy. This poses challenges for other countries, including the UK, on how best to navigate between these different regulatory approaches. Japan for instance has less-stringent data protection

standards than the EU, but it has been able to secure a mutual adequacy agreement by committing to uphold more stringent privacy protections on EU citizens' data than Japanese citizens' data, resulting in a two-track data management regime.[48]

An alliance of smaller, internationally oriented and trade-dependent governments is seeking to promote interoperability between different regimes. In June 2020, New Zealand, Singapore, and Chile agreed a new Digital Economy Partnership Agreement (DEPA) which builds from and refines the CPTPP text (all three countries are members), and sets out new areas for future co-operation, including AI and fintech.[49] The agreement aims to preserve "a free, open, global, and secure internet".[50] The agreement is intended to be a framework for digital trade that other governments can use: DEPA takes a modular approach, and modules are intended to be building blocks. The agreement is open to other countries to join (art. 16.4). Alternatively, governments could slot modules from DEPA into other trade agreements or use them as the basis for aligning domestic policies.[51] Although the three countries have been more closely aligned with a US approach to digital trade than that of the EU and China, there are some notable differences between DEPA and the US approach in recent trade agreements, with DEPA attempting to strike more of a balance between the liberalising drive of the US, and the EU and Chinese demands for regulatory autonomy.

4 Policy issues in detail

In this section we examine five policy areas in detail, broadly following the key themes addressed in digital trade chapters of recent trade agreements:

(1) Cross-border data flows, data localisation, and personal data protection

(2) Internet access and content regulation, including liability of internet companies for online content

(3) IP protection and innovation, including provisions on source code and algorithm disclosure

(4) E-commerce, which focuses on issues of trade facilitation (including e-signatures and authentication, and efforts to promote paperless trading), and consumer protection

(5) Customs duties on electronic transmissions and the implication of non-discrimination provisions for the use of digital services taxes.

We examine how the US, EU, China and selected other countries have approached digital trade in each of the five policy areas, and then examine the UK's emerging position.

4.1 Cross-border data flows, data localisation and personal data protection

This section examines provisions regulating the flow of data across national borders, including provisions on personal data protection, and provisions establishing where data is allowed to be stored.

Overview of policy issues

The regulation of cross-border data flows is a contentious policy issue. Ubiquitous digitalisation and the societal embeddedness of digital media have changed the volume, intensity, and nature of data flows across borders. The value of data, as well as the risks associated with data collection and processing by companies and governments, have dramatically changed. In response, governments have altered the way they regulate cross-border data flows. While a first generation of controls sought to restrict inflows of data, including through censorship of internet content, a new generation of measures seeks to restrict outflows. Restrictions on outflows create frictions for cross-border data flows and the smooth running of digital supply chains, but there are many public policy reasons why governments restrict data transfers, including to safeguard the fundamental rights of their citizens, public interests, and values that matter for their constituencies.[52] In light of concerns about where the economic gains from data accrue, United Nations Conference on Trade and Development (UNCTAD) recently argued that the only way for developing countries to exercise effective economic 'ownership' of and control over the data generated in their territories may be to restrict cross-border flows of important personal and community data.[53] In practice, governments have taken very different approaches – ranging from allowing and promoting the free flow of data to implementing extensive data restriction and localisation measures.

Privacy is a major concern in many countries. Personal data have become a resource that drives much economic activity online, and the way in which personal data are handled and used can raise concerns regarding privacy and the security of information. This has become more evident with recent cases making the headlines, such as those involving Facebook and Cambridge Analytica, and frequent reports of data breaches.[54] These concerns have international dimensions as the global nature of the internet means that personal data can be quickly and easily transferred to parties in other jurisdictions. This transfer can undermine domestic privacy goals when the personal data of citizens flows to jurisdictions that do not offer comparable levels of privacy protection.[55]

In response to increased risks to privacy, governments have updated and adapted their existing personal data protection legislation, regulations, and guidelines, in general moving from measures that react to a breach of privacy to proactive measures to protect privacy. New laws and regulations seek to forestall the risk of personal data being stolen or breached, and to set limits on what personal data can be collected, whether and how consent from the user/consumer is needed, how the data may be used, stored, transferred, or removed. The scope and nature of regulation varies enormously across countries. Some countries protect privacy as a fundamental right, while others base the protection of individual privacy in other constitutional doctrines or in tort. Some governments prevent their citizens' data from flowing to jurisdictions with lower levels of regulatory protection, as the EU has

done with its GDPR. Broadly ratified international treaties protect the right to privacy, such as the International Covenant on Civil and Political Rights and the European Convention on Human Rights, which also apply on the digital realm. Still, a number of countries have yet to adopt legislation, policies or measures to ensure data privacy protection.[56]

In addition to privacy concerns, governments may restrict the flow of data for regulatory reasons, with several countries imposing measures requiring financial data to be stored locally to ensure that regulators can access data for supervisory and regulatory purposes. Governments also require localisation on national security grounds, on the basis that data localisation decreases the risks of unauthorised access. China's Cybersecurity Law for instance, requires data localisation and access to source code for critical information infrastructure. Governments may also restrict data flows to control access to certain types of online content, usually on moral, religious, or political grounds.[57]

The debate in the trade policy world is over the extent to which restrictions and localisation measures are necessary for pursuing legitimate public policy goals or unnecessary barriers to trade. While specific rules on cross-border data flows are now being negotiated at the WTO and in bilateral and regional trade agreements, some older WTO rules do have implications for cross-border data flows. For instance, the GATS Annex on Telecommunications requires governments to allow telecommunication networks and services to transfer data or access databases stored abroad in order to supply services covered by countries' scheduled liberalisation commitments. Similarly, the Understanding on Commitments on Financial Services states that Members shall not apply measures that prevent transfers of information or the processing of financial information (including transfers by electronic means), where such transfers or processing of information are necessary for conducting the ordinary business of a financial services supplier. Finally, data flows can be considered as services in some cases, making the liberalisation commitments under GATS particularly relevant.[58]

Of course, there are 'general exceptions' that apply and provide some flexibilities. Notably Article XIV of the GATS allows WTO Members to adopt measures that would otherwise violate their obligations, so long as these measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services. Article XIV GATS includes two specific categories that are pertinent for cross-border data flows, those relating to public order or public morals and those that are necessary to secure compliance with laws or regulations, including with those relating to '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' (art. XIV (c)(ii) GATS).[59] The core element of the Article XIV exception is the so-called 'necessity' test which requires weighing and balancing different factors, including the extent to which the measure furthers public policy objectives, and the extent to which it impacts trade flows. If the party whose measure is being challenged demonstrates the prima facie 'necessity' of its measure, the claimant can rebut the 'necessity' by demonstrating that a less trade-

restrictive alternative to the measure has been 'reasonably available', meaning that it allows the defending party to achieve the pursued public policy objective without prohibitive costs or substantial technical difficulties to that party.[60]

As no case law has clarified the application of Article XIV(c)(ii) to privacy and personal data protection measures, there is a high level of uncertainty and unpredictability about the extent to which measures used by WTO Members to protect privacy are compatible with their obligations under GATS. Several experts argue that aspects of the EU's GDPR are unlikely to comply with the EU's GATS obligations. Crucially, there are several different alternative approaches to data privacy, including the 2013 OECD Guidelines and the 2015 Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which are arguably less trade-restrictive than the GDPR. The existence of these approaches puts the EU's fundamental rights-based privacy and data protection framework at risk of not passing the necessity test in GATS Article XIV.[61]

US approach in trade agreements

The US is a strong advocate of cross-border data flows and seeks to obtain positive obligations that governments will allow data flows, and to impose limits on the measures that governments can use to regulate data flows, including on the grounds of privacy.

The TPP was the first US agreement with binding positive commitments that Parties "shall allow" transfer of information, and when the US withdrew, this provision was maintained in the CPTPP. The USMCA and US–Japan texts built from the TPP and include binding commitments that "No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person" (art. 19.11 USMCA; art. 11 US-Japan). Such provisions have broad scope: unlike GATS, which only covers data necessary for the provision of services, personal information is explicitly included. As a result, most data that is transferred over the internet is likely to be covered by this commitment, although the word 'for' may suggest the need for some causality between the flow of data and the business of the covered person.[62] The wording in the USMCA and US–Japan is particularly stringent as mere restrictions (for example, governments slowing down or complicating access to data) are now also within scope, not just outright prohibitions.[63] Unlike WTO provisions related to cross-border data flows in financial and telecommunications services, clauses in the USMCA, CPTPP, and other recent agreements are formulated as a positive obligation and are not sector-specific.[64]

Although there is an exception (modelled on GATS Article XIV) in recent US agreements for measures "necessary to achieve a legitimate public policy objective" these must not be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade" and must pass a necessity test as Parties cannot "impose restrictions on transfers of information greater than are necessary to achieve the objective" (eg art. 19.11 USMCA). This provision differs from the WTO norms in one significant element: while there is a list of

public policy objectives in the GATT and the GATS (such as public morals or public order), the USMCA provides no such enumeration and simply speaks of a "legitimate public policy objective." This permits more regulatory autonomy (although it may lead to overall legal uncertainty). There is also a general exception in the chapter for government procurement and data held by government (art. 19.2.3).[65]

The TPP was also the first US agreement containing explicit restrictions on the use of data localisation measures, and again this was retained in the CPTPP. The USMCA also includes a prohibition on localisation: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory" (art. 19.12 USMCA). Unlike the CPTPP, the USMCA provision banning data localisation contains no public policy exception (art. 14.13 CPTPP). Although these commitments are still subject to the general exception provisions of the agreements, these apply GATS Article XIV, as discussed above, and there are concerns that this may not be sufficient to safeguard many of the regulatory measures that governments use to protect privacy.[66] In Canada for instance, which is a signatory to the USMCA, there are concerns that data localisation requirements taken by British Columbia and Nova Scotia to keep sensitive health information at home may not be in line with Canada's obligations under USMCA.[67] The prohibitions on localisation measures in US agreements are also qualified with regards to financial services.[68]

The US approach to personal data protection in its trade agreements reflects its domestic policies. Unlike the EU, the US does not have a single data protection law with 'omnibus' coverage. Rather, the sectoral, federal, and state laws are a patchwork governing dimensions of privacy and data protection that have not been translated into a robust body of case law extending the right to privacy into a comprehensive right to personal data protection.[69] US laws contain minimal guarantees of an individual's right to not have confidential personal information exposed online, but US laws do not require companies to get informed consent to use personal data, nor do they establish a baseline commercial data privacy framework. While there are specific statutes on data protection in areas such as health, they do not cover many business sectors such as banks, airlines, insurance, and common carrier activities of telecommunications service providers. In these sectors, a mix of legislation and self-regulation allows companies and industry bodies to establish codes of practice on the assumption that the market will do a better job at reaching a balance between commercial needs and privacy interests.[70] Some individual states have created specific data protection laws, notably the recent California Consumer Privacy Act which is more comprehensive and applies to online business. Although there have been moves to introduce stronger data protection legislation at the federal level, these have not been successful.

US trade agreements do include stand-alone articles on the protection of personal information, but they are nowhere near as robust as the provisions advocated by the EU (discussed below). USMCA contains a stand-alone article on the protection of personal information (art. 19.8 USMCA), and there is an analogue provision in CPTPP (art. 14.8 CPTPP). Unlike the EU's approach, which completely carves out privacy measures from the scope of the agreement, in US agreements there is simply a

binding commitment to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade" and the Parties agree to extend the scope of domestic privacy law to personal data collected from people located overseas.[71] Parties "shall endeavour" to adopt measures that are non-discriminatory (art. 19.8.4 USMCA), publish information on remedies and on how enterprises can comply (art. 19.8.5 USMCA), and co-operate to promote compatibility between personal data protection regimes (art. 19.8.6 USMCA). US trade agreements also stop short of specifying minimum standards for privacy protection, simply stating that Parties "should take into account principles and guidelines of relevant international bodies" (art. 19.8.6 USMCA).

Moreover, US agreements explicitly recognise that the APEC Cross-Border Privacy Rules (CBPR) system is a valid mechanism to facilitate cross-border information transfers while protecting personal information (eg art. 19.8.6 USMCA) and Parties agree to work together to promote the APEC rules (art. 19.14 USMCA).[72] Thus, while the USMCA text acknowledges that there are different approaches to personal data protection, the Parties explicitly endorse industry self-regulation and the relatively light-touch APEC rules as sufficient mechanisms for protecting personal information.[73] USMCA also includes a necessity test, which stipulates that any restrictions on cross-border flows of personal information must be "necessary and proportionate to the risks presented" (art. 19.8.3 USMCA). Very similar provisions are found in the US–Japan agreement, although the provisions stop short of explicitly endorsing the APEC approaches (art. 15 US–Japan). Crucially, the drafting of recent US provisions on privacy appear to rule out the EU's GDPR as unduly restrictive. In particular, by explicitly endorsing the much less stringent APEC rules as sufficient for protecting personal information, it is hard to see how the EU's GDPR would pass the necessity test.

EU approach in trade agreements

On cross-border data flows, the EU has taken a very different approach to the US, and has only recently begun to negotiate provisions in its trade agreements. In the EU–Japan and the modernisation of the trade part of the EU–Mexico Global Agreement (hereafter 'EU–Mexico'), Parties merely agree to consider commitments related to cross-border flow of information in the future. In the EU–Japan agreement, Parties commit to "reassess" within three years of the entry into force of the agreement, the need for inclusion of provisions on the free flow of data into the treaty (art. 8.81 EU–Japan). There is no provision in the EU–Japan or EU–Mexico agreements on data localisation.

The EU's hesitancy to agree to commitments to facilitate cross-border data flows stem in a large part from its approach to personal data protection. In the EU, privacy and personal data of citizens and residents are protected as fundamental rights.[74] The GDPR,[75] which entered into force in 2018, applies to all personal data processors in the EU, both public and private actors, and to EU citizens data anywhere in the world. The regulation establishes a number of legal guarantees to data subjects, including the right to access information about them, and the right to have such

information corrected or deleted. Under the GDPR, firms have to clearly specify how data about individuals are being used, and they must ask for prior consent to collect and use the data. All this is backed by enforcement mechanisms, including significant fines for non-compliance. Several other countries have adopted or are considering the adoption of similar data protection rules, including Brazil, India, Japan, and the Republic of Korea.

As explained above, rather than turn to trade agreements, the EU has relied on its market power and the extraterritorial reach of its legislation to ensure that its citizen's data is adequately protected in other jurisdictions. Since EU efforts to achieve its privacy goals can be circumvented when data are sent to other jurisdictions with lower levels of privacy protection, the GDPR makes it illegal to transfer data outside of the EU unless privacy is adequately protected in the data destination country, including with respect to the rights of the data subject. In practice this has meant a privacy regime that is judged to be equivalent to that of the EU and the adequacy standard does not require a point-to-point replication of EU rules, as confirmed by the CJEU.[76] The EU unilaterally decides whether other jurisdictions are deemed to offer adequate protection, issuing adequacy decisions that apply to the whole jurisdiction or, in the case of 'partial' adequacy decisions, to specific sectors or industries.[77] In the absence of an adequacy decision, the EU allows data to be transferred internationally using model contracts (standard contractual clauses) that effectively bind the recipient of the data to privacy protection equivalent to that if the data had remained in the EU. Personal data can also be transferred across borders within a single company if that company has accepted binding corporate rules on privacy.[78] This means that the jurisdiction of the GDPR effectively has a global reach.[79]

Notably, the US currently does *not* have an adequacy decision in place. Until recently, data flows have been managed through the US–EU Privacy Shield. However, in July 2020 the CJEU invalidated the US–EU Privacy Shield (Schrems II*)*.[80] Among the reasons articulated were concerns with the lack of safeguards surrounding government access to personal data transferred from the EU for the purposes of law enforcement and national security.[81]

The Schrems II ruling also makes it harder for companies to turn to standard contractual clauses and binding corporate rules, the other mechanisms under the GDPR for transferring personal data out of the EU, by requiring additional safeguards that are not readily available.[82] The Court held that standard contractual clauses remain valid where the Parties put in place 'additional safeguards' such as encryption and pseudonymised data, and this would also require that the data cannot be decrypted by national security agencies. The decision emphasised that data controllers are expected to verify that the level of protection afforded by the country of destination is adequate in order to make use of standard contractual clauses.[83] It also requires data protection authorities to determine the suspension of data transfers to any country where EU standards are not met. But some analysts argue that making such an assurance would require knowledge of the capabilities of other countries' national security agencies that is so unrealistic as to make such additional safeguards unavailable for most, if not all, businesses.[84]

Having historically eschewed the inclusion of provisions on cross-border data flows in its trade agreements, the EU's position shifted in 2018, when the European Council agreed to new language that the EU would propose in its trade agreements that aims to support free flow of information while also safeguarding the privacy of citizens. The EU's proposals have two core components:

- to prohibit specific types of restriction on cross-border data flows, rather than a broad commitment to allow cross-border flows
- to include an extensive exception for privacy, which completely carves out privacy measures from the scope of the agreement.

The aim of these provisions is to promote cross-border data flows while ensuring that the EU unconditionally preserves its autonomy to regulate in the interest of data privacy, so that the GDPR is immune from challenge.[85]

This position was reflected in the EU's proposals in negotiations with the UK, where it proposed that Parties should recognise privacy as a fundamental right and include an unconditional, self-judging exception stating: "Each Party may adopt and maintain the safeguards *it deems appropriate* to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data" and that "Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards" (art. DIGIT.7 in EU proposal).[86] Crucially, unlike the exceptions in GATS and in USMCA discussed above, under the EU proposal there would be no requirement for Parties to show that the measure is 'necessary', non-discriminatory, and least trade-restrictive.

The EU has proposed similar text in the trade negotiations with Chile, Indonesia, Mexico, New Zealand, and Tunisia and is planning to replace the '*rendez-vous*' clause in the EU–Japan and EU–Mexico agreements with the new position.[87] It is also reflected in the EU's proposal for the ongoing WTO negotiations on trade-related aspects of e-commerce.[88]

During EU–UK negotiations, the UK agreed to the first but not the second element of the EU's approach. The Parties agree to a list of specific data flow restrictions that will be prohibited, including "requiring the use of computing facilities or network elements in the Party's territory for processing", "requiring the localisation of data in the Party's territory for storage or processing", "making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory" (art. DIGIT.6 TCA). The list of prohibited measures will be kept under review. Unlike US agreements, the Parties do not make a positive commitment to allow free-flow of data.

On personal data protection, the Parties avoided the use of the term "fundamental right" and instead recognise that "individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade" (art. DIGIT.7 TCA). Instead of an unconditional, self-judging exception, the final EU–UK text states: "Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the

protection of personal data and privacy, including with respect to cross-border data transfers, *provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred*" (emphasis added) where "conditions of general application" refer to "conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases" (art. DIGIT.7 TCA). In line with EU proposals, the TCA carves out issues of cross-border data flows and the protection of personal data from the dialogue on regulatory co-operation with regard to digital trade (art. DIGIT.16 TCA). While the TCA provisions are less expansively drafted than the EU's initial proposals, they provide far greater regulatory autonomy than recent US agreements as privacy measures are not subjected to any trade-related tests, and provide an indication of the type of provisions that the EU is prepared to accept.

China's approach in trade agreements

The Chinese government imposes a series of restrictions on cross-border data flows and, for this reason, it has avoided making commitments on cross-border data flows in its trade agreements. For instance, the government blocks sites by IP address and blocks and filters uniform research locators (URLs) and search engine results. It also requires data to be localised. China's Cybersecurity Law, which took effect in June 2017, requires firms operating in China to store data collected in China to be kept on servers located in the country. Any publisher of online content must locate their "necessary technical equipment, related servers and storage devices" in China; firms and individuals storing and processing personal, financial, and population health information must store the data in China; and online maps must be kept on a server inside China. A significant portion of data cannot be transferred outside of the country without official approval, following a security assessment. Finally, foreign firms cannot offer cloud-computing services without a Chinese partner owning at least 50% of the joint venture.[89]

Until recently, the protection of personal data was not a priority. The term 'right of privacy' did not even exist in Chinese laws and regulations before the end of 2009, when the Tort Liability Law was enacted, and this law does not affect public law. Moreover, the government has established many exemptions that give it extensive rights and generous room for flexibility for investigation, seizures and search, especially in the areas of state security or for maintaining social order. For instance, the State Security Law, enacted in 1993, allows Chinese security institutions to access "any information or data held by an entity in China whenever they deem it necessary". The Chinese government has shared personal data with firms and vice versa, enabling data economies of scale and scope, and helping firms to develop AI.[90] However, Chinese citizens have become more concerned with online privacy, and in October 2020 the government released a draft Personal Information Protection Law, the country's first comprehensive legislation on personal data protection, which has strong resemblances to the EU's GDPR.[91]

Given China's interventionist approach to data regulation, it is unsurprising that neither the China–Korea agreement nor the China–Australia agreement contain provisions on cross-border data flows or data localisation. Provisions are found in RCEP, although they provide a high level of flexibility. Parties agree "not to prevent" cross-border transfers, although inconsistent measures are allowed if they are "necessary" in order to achieve a "legitimate public policy objective" (art. 12.15 RCEP). Unlike US agreements, the decision on whether a measure is necessary is self-judging, and although a Party could be challenged on whether the public policy objective is legitimate, the provisions are not subject to the dispute settlement chapter. Measures must not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade. However, unlike US agreements, there is no requirement that the measure be "least burdensome" to achieve the objective. In addition, the obligations are subject to a completely self-judging and non-disputable national security exception – a Party can adopt any measures it considers necessary for its essential security interests, and such measures cannot be disputed by the other Parties (art. 12.15 RCEP). The provision on data localisation is similarly crafted. A covered person cannot be required to use or locate computing facilities, such as servers, in a Party's territory as a condition of doing business there, although this commitment is subject to the same exceptions as the commitment on data flows (art. 12.14 RCEP).

There is a provision on online personal information protection in the draft RCEP agreement (art. 12.8 RCEP). Parties commit to a legal framework that "ensures the protection of personal information of the users of electronic commerce". There is no minimum standard, although a Party must "take into account" international standards, guidelines, and so on, of relevant international bodies. As with the similar provisions in the USMCA, US–Japan and CPTPP, a footnote stipulates that Parties can comply by adopting a comprehensive personal privacy law or sector-specific laws, or by providing for enforcement of contractual obligations that enterprises adopt (art. 12.8 RCEP) but, unlike USMCA, there is no explicit endorsement of the APEC rules.

DEPA

With regards to cross-border data flows, the DEPA approach is modelled on the CPTPP provisions, which is unsurprising as the three members of DEPA are also members of CPTPP. The DEPA text on data flows and data localisation simply repeats the CPTPP provisions, which, as explained above, commit the Parties to allowing cross-border data flows and ban data localisation measures, although both are subject to an exception for "legitimate public policy" measures that pass a necessity test (art. 4.3 and 4.4 of DEPA). The DEPA contains a provision on personal information protection that is similar to provisions found in the CPTPP. However, it is slightly more extensive, setting out principles that should underpin a "robust legal framework" for the protection of personal information, and it encourages the use of data protection trustmarks (art. 4.2 DEPA).

UK approach in trade agreements

A key decision for the UK is whether, and to what extent, to stay aligned with the EU's approach to data regulation. There have been signals that the UK is seeking to move away from the EU's approach and adopt a more liberalising stance. The government's new National Data Strategy includes a mission to "champion the international flow of data" and the UK Prime Minister has indicated that data protection standards in the UK are likely to diverge from the GDPR after Brexit.[92]

The strongest sign that the government's approach is shifting is found in the UK–Japan free trade agreement, where the digital trade provisions are based on the CPTPP (to which Japan is a signatory).[93] The UK–Japan agreement adopts the CPTPP text for provisions on cross-border data flows (art. 8.84 UK–Japan), data localisation (art. 8.85 UK–Japan), and privacy (art. 8.80 UK–Japan), with very minor revisions.[94] This suggests that the UK is heading broadly in the direction of the US approach to regulating cross-border data flows and privacy. Rather than providing for an EU-style prohibition on specific data flow restrictions, and a complete carve-out for privacy measures, the UK makes a general binding commitment to data flows and treats privacy as one possible consideration in the "legitimate objective" exception. While Parties commit to upholding personal data protections, the UK–Japan agreement does not set minimum standards. Notably, the UK commits in the UK–Japan agreement to maintain privacy standards that will meet the tests of not imposing restrictions on transfers of information that are "greater than are required to achieve the objective" (art. 8.80 UK–Japan). The UK government has stated that its commitments in the UK–Japan agreement are commensurate with its aims of upholding high standards of privacy under the UK's Data Protection Act 2018.[95] However, as discussed in previous sections, it is far from clear that the GDPR (to which the UK currently adheres) would meet the necessity test stipulated in the UK–Japan agreement.

The UK needs to be careful in departing from the EU's approach to cross-border data flows and privacy, as it has a delicate balancing act to strike, particularly as it is seeking an adequacy decision from the EU. While other countries with data protection systems that are different to the GDPR have obtained an adequacy decision, including Japan, obtaining adequacy is not straightforward.

At the time of writing, the UK has conferred adequacy on the EU on a transitional basis, allowing personal data to flow from the UK to the European Economic Area (EU countries plus Iceland, Liechtenstein and Norway) for a few years while the UK undertakes its own adequacy assessments.[96] However, the EU is yet to confer adequacy on the UK. Instead, the recent EU–UK trade agreement provides a six-month window during which data can flow from the EU to the UK pending the outcome of the EU's adequacy decision, so long as the UK stays aligned with the EU GDPR.[97] Obtaining adequacy is extremely important for businesses, and a recent study suggests that not obtaining EU adequacy would cost UK businesses between £1 billion and £1.6 billion in additional compliance costs.[98] The government has stated that it is also "extremely important" for effective UK–EU co-operation in law enforcement.[99]

To obtain adequacy, UK data protection standards must remain equivalent to those provided by the GDPR. As the UK's Data Protection Act 2018 is based on the EU's GDPR, as is the UK's international data transfers framework, obtaining adequacy would appear straightforward. However, experts have flagged several factors that make the adequacy decision less certain. Following the UK's exit from the EU Charter of Fundamental Rights, there is no equivalent to Article 8 (on data protection) in UK law, so data protection is no longer a fundamental right of UK citizens, providing a lower level of legal certainty regarding the extent to which personal data will be protected.[100] The recent ruling by the CJEU invalidating the US–EU Privacy Shield (Schrems II) introduces some complexities now that the UK is no longer an EU member state.[101] Crucially, Schrems II revealed that the CJEU is prepared to provide greater flexibility to EU member states in balancing rights to privacy and security than third countries like the US.[102] Although the UK's surveillance practices haven't changed with its exit from the EU, in the wake of Schrems II, specific powers granted to government ministers under the UK Investigatory Powers Act 2016 may create challenges.[103] When reviewing the UK request, the European Commission is likely to more closely scrutinise UK investigatory powers and the legal conditions under which data from communications can be held and transferred to intelligence agencies.[104]

A further concern arises from commitments that the UK is likely to enter into in trade agreements on the free flow of data with third parties like the US, which do not have stringent regulations on personal data protection. To obtain (and maintain) an EU adequacy decision, countries must have in place effective mechanisms to ensure that EU citizen's data is not transferred to another third country (an "onward transfer") unless protections are in place that guarantee the required level of protection. For example, the EU's adequacy decision on Japan stipulates that EU citizen's personal data cannot be automatically transferred to third countries through APEC Cross Border Privacy Rules as protections are "clearly of a lower level".[105]

Whether the arrangements needed to secure adequacy decisions are consistent with commitments in free trade agreements that provide for free flows of data is complex and contested. Some privacy scholars argue that if a country "commits to free cross-border data flows in a free trade agreement with yet other countries, it is risking its strategic ability to obtain a finding of adequacy by the Commission".[106] Indeed, according to the European Data Protection Board (which leads on adequacy assessments for the EU) any agreement concluded between the UK and the US would have to be taken into account when assessing the level of protection of personal data in the UK, in particular to ensure continuity of protection in case of onward transfers.[107] However Japan has obtained an adequacy decision from the EU, even though it has entered into commitments in trade agreements on free flow of data, including with the US. This is due to what one expert calls a "work-around" as Japan has created a two-tier data protection regime with different arrangements for personal data originating from the EU and from within Japan, including in the area of onward transfers.[108] Experts disagree on whether such arrangements are legally consistent with commitments in trade agreements on free data flows.[109]

These points notwithstanding, other experts argue that the EU is highly likely to grant the UK adequacy. As the UK is a departing EU Member State, deciding that the UK is not adequate would set the bar for adequacy impossibly high, and could create substantial difficulties for the EU in conferring new adequacy decisions, and prove a barrier to continuing existing adequacy decisions which are being reviewed by the European Commission.[110] It is possible that the EU confers adequacy (a decision made by the European Commission following a recommendation from the European Data Protection Board, and approved by EU Member States) but this is later invalidated by the CJEU, as happened to the EU–US Privacy Shield. If this were to happen, the law enforcement provisions in the new UK–EU trade agreement contain explicit clauses that enable certain provisions in the law enforcement context to be suspended. For instance, the EU could explore ways to postpone the entry into effect of the Court's decision, reduce its scope or withdraw it.[111]

In sum, the UK may well be able to follow Japan's lead and create workarounds that enable it to maintains EU adequacy while also committing to the free flow of data in trade agreements with third countries, essentially by guaranteeing that it will afford levels of protection for EU citizens' data that are in line with GDPR. The most pressing issue for the UK is to establish the level of personal data protection that it wishes to uphold for its own citizens, and to ensure that its data protection arrangements are immune from challenge under its trade agreements. The available evidence certainly suggests that the type of privacy exceptions found in the UK–Japan agreement, the CPTPP, and recent US agreements may not be sufficiently robust to safeguard the UK's own GDPR and adequacy arrangements in the event of a legal challenge.

4.2 Internet access and content regulation

This section discusses the rules and regulations in trade agreements that have implications for the regulation of the internet, both with respect to regulating access to networks and regulating online content, including the liability of internet platforms.

Overview of policy issues

In terms of access to the internet, trade agreements often include network management rules to safeguard equal and non-discriminatory treatment of internet traffic. These rules promote the principle of network neutrality, which requires broadband providers to treat all users, websites, and services equally.[112] The goal is to protect an open and innovative internet, preventing network managers from blocking or throttling (intentional slowing or speeding of internet traffic) lawful connections, and from censoring, filtering or charging more for specific contents.[113] Network neutrality also promotes competition in digital markets, levelling the playing field and ensuring that content and services from small and big businesses are treated equally.

Countries have adopted different network neutrality rules domestically. In the US, the Federal Communications Commission (FCC) changed the rules on the classification of internet service providers in 2017, which *de facto* repealed the principle of

network neutrality in the country.[114] In contrast, the EU actively promotes network neutrality via the Open Internet Regulation, which establishes that users have the right to "access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service". In light of Brexit, the UK has chosen to retain the EU regulations via the UK Open Access (Amendment Etc) (EU Exit) Regulations 2018 and housed them under the supervision of Ofcom, the telecommunications regulator.[115]

In terms of the regulation of internet content, internet platforms that host user-generated content, such as Facebook, YouTube and Twitter, are usually considered intermediaries and not publishers of such content. From a public policy perspective, concerns remain as to whether and how these companies should be legally responsible for online harms (including child pornography and hate speech) and rights violations (including copyright infringement) caused by the content they host. To address these issues, governments have developed intermediary liability rules. These rules typically have three main policy goals. The first is to protect internet users and prevent harms and criminal activity online; the second is to promote fundamental rights such as free expression and information access; and the third is to protect businesses and encourage economic growth and technical innovation. Balancing these objectives has proven complicated and there has been growing pressure on governments, including in the UK, US, and EU, to revisit their domestic legislation on intermediary liability.

Experts largely disagree on the best way to approach intermediary liability and on how to strike the delicate balance between the relevant public policy objectives at stake, both with regards to general liability rules and to rules specifically developed to address IP violations. Governments around the world are under pressure to clamp down on online harms and the online dissemination of illegal content. At the same time, there are legitimate concerns regarding the procedures required to enforce some regimes of intermediary liability, and the impact they could have on internet content moderation. Experts worry that some liability models would provide incentives for platforms to use filtering tools and adopt review procedures that are more likely to censor legitimate speech, with chilling effects for freedom of expression online and access to information.[116]

US approach in trade agreements

In the US, the main rules on intermediary liability are laid in section 230 of the US Communications Decency Act (CDA), which limits the liability of internet companies that host user-generated contents, such as Facebook and Twitter, for the behaviour of their users. Adopted in 1996, CDA s. 230 is now highly contentious.[117] Some experts, policymakers and interest groups argue that CDA s. 230 provides a blanket waiver that permits tech companies to get away with not moderating harmful content sufficiently, in turn allowing hate speech and other forms of harassment on their platforms.[118] Others believe it permits too much content moderation – allowing

online platforms to suppress so-called 'conservative speech'. Technology companies, in turn, argue that the current provision is crucial to ensuring competition and freedom of expression on the internet.[119] Some of these concerns are shared by scholars and civil society organisations, who see s. 230 as a cornerstone of free internet speech.[120]

A series of proposals in the US aim to change CDA's liability regime, and newly inaugurated President Joe Biden has previously suggested that s. 230 should be revoked.[121] However, there is no consensus on how exactly intermediary liability rules should be changed. Under the Trump administration, moves have been made to limit private companies' ability to set the rules on content moderation. In 2019, the Senate introduced a bill to prohibit large social media companies from moderating "politically biased" information on their platform.[122] Criticisms of s. 230 also underlie the executive order issued by President Trump on "Preventing Online Censorship" on May 2020. In September 2020, the Department of Justice sent draft legislation to Congress to execute the presidential directive and to reform the CDA.[123] In November 2020, executives of Twitter and Facebook were called to testify before the Senate Judiciary Committee, which is currently considering s. 230 reforms.[124] The proposed amendments would change liability rules and also limit the broad immunity enjoyed by internet platforms for content moderation decisions made in "good faith".

The liability of internet platform for infringements of IP rights (including copyright) are usually governed by specific rules, which represent an exception to the general intermediary liability regime. In the US, the Digital Millennium Copyright Act (DMCA), adopted in 1998, introduces an exception to the CDA regime that applies to online service providers in cases of copyright violations. Section 512 of the DCMA establishes that, as long as online service providers comply with certain requirements and block access to alleged infringing material upon receiving notification of an infringement, they are protected from liability – the regime known as "notice and take down". In practice, it gives stronger protection to allegations of copyright infringement than to allegations that would fall within the general scope of the CDA. Under the DMCA s. 512, users based anywhere in the world are able to send notifications to US-based companies reporting copyright violations and asking for the removal of content. This mechanism has also been used beyond the original scope, including the removal of non-consensual intimate images (also known as 'revenge porn')[125] and, worryingly, been employed by authoritarian governments to censor critical voices online.[126] In May 2020, the US Copyright Office issued a detailed study on s. 512, which concluded that the operation of the section 512 safe harbour system is "unbalanced", and called for changes that would "better balance the rights and responsibilities of online service providers and rightsholders in the creative industries".[127]

Internet access provisions found in recent US agreements (including the USMCA) make no binding commitment to network neutrality. Rather, they recognise the benefits of access and use of internet services, subject to "reasonable network management", without further details on the circumstances that would allow such

management. This is unsurprising, considering that the US domestic regime does not actively promote network neutrality domestically, as discussed above.

In relation to intermediary liability, the USMCA was the first US agreement to include provisions explicitly modelled on the contentious section CDA s.230 (art. 19.17.2 USMCA).[128] The agreement was ratified and implemented while a heated debate regarding the efficacy of ISP liability safe harbours was unfolding domestically in the US, with calls to overhaul the regime under CDA s.230, as discussed above.[129] This led experts to argue that internet companies lobbied for the inclusion of this provision in the agreement to protect against domestic reforms.[130]

With regards to copyright infringements, the USMCA includes a provision that mirrors DCMA s. 512. Article 20.88 of the USMCA, which requires Parties to establish appropriate safe harbours for internet platforms, including incentives for companies to remove or deter access to illegal content, and the adoption of a 'notice and take down' mechanism. An identical provision is found in the CPTPP, which requires Parties to require internet service providers to "expeditiously remove or disable access to material residing on their networks or systems upon obtaining actual knowledge of the copyright infringement" (art. 18.82 CPTPP). The USMCA was approved while domestic debates were unfolding domestically in the US on whether safe harbours provide sufficient protection to copyright holders. The inclusion of a provision modelled on DCMA s. 512 in the agreement has led the leaders of the Congressional House Judiciary Committee to write to the US Trade Representative to request that Article 20.88 be dropped from the USMCA and future trade agreements "while such serious policy discussions are ongoing".[131]

EU approach in trade agreements

The EU makes stronger commitments to protecting network neutrality in trade agreements than the US. In contrast to the US, the EU has largely refrained from including liability provisions in trade agreements, and when it has, they are less prescriptive than the US provisions, and restricted to copyright infringements. Consequently, the EU has largely preserved its regulatory autonomy with regards to conducting domestic reforms in the liability regime.

Liability of internet platforms in the EU is currently regulated by the e-Commerce Directive, adopted in 2000, which provides for a safe harbour regime for intermediaries. Under the e-Commerce Directive, internet intermediaries – classified as mere conduit, caching, or hosting platforms – should not be held liable for content hosted by them when they do not have knowledge that the content they host is unlawful, or when they act quickly to remove or to disable access to the information once they are aware of its illegality.[132] This regime is due to be replaced by the DSA, which will introduce a new set of rules for online intermediaries and platforms.[133] DSA-proposed obligations will apply asymmetrically (that is, they will vary according to the characteristics, size, and social impact of the service provider), and not only to internet intermediaries operating in the EU, but also to those established in third countries that offer services in the European Single Market. The new framework will require platforms that host user-generated content to

implement a 'notice-and-action' mechanism, so that users can notify online intermediaries about potentially illegal online content or activities, but which largely preserves the same liability exceptions listed in the e-Commerce Directive.[134] Importantly, the DSA does not introduce active monitoring obligations that have been criticised by stakeholders concerned with free speech.[135]

The EU recently adopted a new liability regime for copyright infringement in the Directive on Copyright in the Digital Single Market, approved in 2019. The legislation introduced a distinction between 'online content-sharing service providers' and other online service providers,[136] removing content-sharing providers (including platforms such as YouTube or Facebook) from the scope of the E-Commerce Directive safe harbours. Under the new rules, content-sharing platforms are required to play a more active role in preventing copyright infringement and should obtain prior authorisation from the right holders (eg a licence agreement) to make content available.[137] In the absence of such authorisation, content providers can be held liable for unauthorised acts of communication to the public, unless they use their "best efforts" to obtain such authorisation and to ensure that copyrighted works are not available on their platforms. The new directive also requires platforms to remove content from their websites upon receiving notice from rights holders, and to employ their best efforts to prevent future uploads of such content, introducing a regime akin to the DMCA 'notice and take down'. Some critics argue that the new rules introduced by the Copyright Directive go beyond the US rule and creates a *de facto* obligation to develop upload filters and other technical tools for content moderation, which are likely to be adopted globally (another example of the so-called 'Brussels effect'). There are also concerns that the new liability rules will further concentrate digital markets, creating a compliance burden that disproportionally affects smaller platforms.[138]

In its joint statement to the WTO, the EU has defended its policy that Members should adopt measures to ensure that users' access to the internet is subjected to reasonable and non-discriminatory network management.[139] Similarly, the EU–Mexico agreement commits Parties to ensure limited, transparent and non-discriminatory network management (art. 10, Chapter on Digital Trade).

With regards to internet content regulation, the EU–Canada agreement includes provisions on liability that are restricted to IP violations. Article 20.11 of CETA requires Parties to adopt limitations or exceptions regarding liability of intermediary service providers for infringements of copyright on the internet. Such exceptions should cover, at a minimum, hosting platforms for content provided by users, caching, and platforms that act as "mere conduits". CETA does not prescribe a notification system, leaving each Party to establish appropriate procedures for effective notifications of violations of copyright.

China's approach in trade agreements

In China, both internet content and internet access are heavily regulated. The government plays a leading role in the management of the internet traffic, and adopts filtering and throttling (the intentional slowing or speeding of internet traffic)

mechanisms that limit access to services and websites considered illegal by the Chinese Communist Party.[140] There are strict liability rules that apply to almost all types of internet service provider. Companies are required to adopt content moderation mechanisms and filtering technologies to promptly detect and block the dissemination of illegal content, and to provide technical support and assistance when requested by government authorities.[141] In 2010, China's State Council Information Office published the country's first white paper on internet policy, which lists a wide range of topics that are considered illegal content and not allowed to be shared online, including content that "subverts state power, undermines national unity, harms national honour and interests" among others.[142] In 2014, China established the Cyberspace Administration of China, the primary regulator for online content, which has issued a number of regulations to tighten the grip on internet content.[143] In 2017, China's Cybersecurity Law came into force, requiring online service providers to verify the real names of users and network operators, and to monitor and flag illegal user-generated content.[144]

Intermediary liability for IP infringement was first regulated in China in 2006, via the Regulations for the Protection of the Right of Communication through the Information Network. The regulation establishes that network service providers can be eligible for safe harbours if they remove or disconnect the link to copyright infringement material upon receipt of a notice and takedown request from a rights-holder.[145] Network providers that provide storage space are not liable if they do not know, or have no reasonable grounds to know, that the material they host infringe another person's rights.[146]

Given China's unique approach to internet regulation and the limitations imposed on what type of services and content Chinese citizens can have access to, it is unsurprising that neither the China–Korea agreement nor the China–Australia agreement contain provisions on intermediary liability or network neutrality. Provisions on enforcement of IP rights in the digital environment are found in RCEP, although they do not establish a special regime for internet platforms. The agreement merely establishes that the same civil and criminal remedies that apply offline shall be available with respect to acts of infringement of copyright or related rights and trademarks online (art. 11.75 RCEP).

DEPA

There are no requirements to explicitly protect network neutrality under DEPA, but Parties recognise the benefits of users being able to access and services and applications "subject to reasonable network management" (art. 6.4 DEPA). Intermediary liability and copyright infringement are not covered in the agreement; the Parties merely agree to "endeavour to cooperate to advance collaborative solutions to global issues affecting online safety and security" (art. 5.2 DEPA).

UK approach in trade agreements

In the UK, the Online Harms White Paper (OHWP), published in 2019, outlined plans to legislate a package of measures aimed at protecting internet users against harms, with a particular focus on children and other vulnerable groups.[147] After a period of consultation, the government's full response to the OHWP was published in December 2020.[148] Among the legislative changes proposed in the response was the introduction of a statutory duty of care for internet companies, under the supervision of Ofcom, requiring platforms to take action to prevent the proliferation of illegal content and activity online. Differentiated obligations will be established depending on type of content (content that is illegal; harmful to children; and legal when accessed by adults but which may be harmful to them) and the reach of the services provided. The majority of services will be required to take action against illegal content and activities, and protect children; while high-risk, high-reach services will be required to take additional action in respect of content or activity that is legal but harmful to adults.[149] Scholars and civil society organisations have claimed that the proposed framework could be unfit to tackle the wide range or of problematic content and behaviour it aims to address,[150] and have voiced concerns that it would threaten fundamental rights, in particular the right to freedom of expression online.[151]

In trade agreements, internet regulation provisions recently agreed by the UK represent a blend of approaches adopted by the US and the EU in previous agreements, and overall tend to be more protective of the interests of businesses than of the interests of individuals.

Regarding the regulation of internet access, the UK–Japan text requires Parties to adopt or maintain appropriate measures to ensure that consumers can access and use internet services and applications, "subject to reasonable, transparent and non-discriminatory network management" (art. 8.78 UK–Japan). This provision was absent from the EU–Japan agreement, but is in line with recent proposals from both the UK and EU in the context of a UK–EU future agreement (eg art. 18.12 of the UK proposal to the EU) and provides a more robust protection of network neutrality by limiting the situations under which network management would be allowed. Network neutrality is likely to be a more contentious consideration in upcoming negotiations with the US. The UK Government has recognised the "value in upholding the principle of fair, transparent and non-discriminatory access for UK telecommunications service providers" in its negotiation objectives with the US. The US, in contrast, did not include provisions related to network management among its negotiation objectives.

In terms of regulation of internet content, the final text of the UK–Japan, similar to the EU–Japan agreement, did not include general provisions on intermediary liability. General provisions on internet intermediary liability are also absent from the UK–EU TCA. The TCA does include a commitment to adopt measures requiring suppliers of goods and services to provide consumers with information and means of redress for breaches of their rights (art. DIGIT.13.1), but does not detail the mechanisms of enforcement. The absence of such provisions from new trade agreements with

Japan and the EU could be a sign of cautiousness from the UK Government, since there is currently no domestic consensus on which liability model the UK should adopt.[152] Following the presentation of the OHWP response at the end of 2020, the government reiterated its commitment to tackling online harms and stated it will carefully consider any interaction between trade policy and online harms policy in future trade agreements. The UK government has claimed that the TCA was specially tailored "preserve policy space for the UK or the EU to protect users online."[153]

The UK–Japan agreement, however, does include novel rules on intermediary liability with regards to violation of IP rights, which were absent from the EU–Japan agreement. It requires Parties to take appropriate measures to limit the liability of online service providers for violation of IP rights where such providers "take action" to prevent access to infringing material in accordance with the laws and regulations of the Party (art. 14.59.2 UK–Japan). This standard provides incentives for Parties to adopt 'notice and takedown' mechanisms, as explained above. The UK–Japan text does include language establishing that Parties shall endeavour to enforce this standard in a way that preserves fundamental principles such as "freedom of expression, fair process, and privacy", but unlike the liability rule, this provision is drafted as a procedural obligation.[154]

With regards to UK negotiations with the US, the published negotiation objectives point to a potential conflict over intermediary liability and internet content regulation. While the UK explicitly mentioned the aim to "promote appropriate protections for consumers online and ensure the Government maintains its ability to protect users from emerging online harms",[155] the US has declared the wish to adopt rules to limit civil liability of online platforms for third-party content in cases unrelated to IP rights. The US is prepared to consider exceptions for "for legitimate public policy objectives or that are necessary to protect public morals".[156] If limits to liability are included in a UK–US FTA, depending on the design of such rules, they could derail the duty of care model proposed in response to the OHWP,[157] and also hinder alternative proposals to improve platform governance, such as enhanced 'procedural accountability.'[158]

Other countries have faced difficulty in navigating between the different EU and US approaches. For example, both Canada and Mexico are Parties to the USMCA despite having domestic liability regimes that do not match the liability regimes modelled in US legislation. Canada does not currently have any statutory measures limiting the civil liability of third-party intermediaries akin to USMCA article 19.17 or CDA s. 230, and existing Canadian common law on defamation is inconsistent with article 19.17.2.[159] In practice, recent rulings by the Supreme Court of Canada have stopped short of holding internet companies liable for harms relating to content posted by someone else, opting instead to pursue equitable relief, and this is an approach that is compatible with USMCA.[160]

Recent proposals to reform Canada's regulations are likely to be inconsistent with Canada's international legal obligations under the USMCA. For instance, in its policy platform released during the 2019 Canadian general election campaign, the

governing Liberal Party proposed to "move forward with new regulations for social media platforms, starting with a requirement that all platforms remove illegal content, including hate speech, within 24 hours or face significant financial penalties."[161] Such a proposal seeks to treat online platforms as an information content provider in determining liability for harms related to information that they took no part in 'creating' or 'developing'. This treatment, however, could be considered inconsistent with USMCA article 19.17.2.[162]

In Mexico, there is currently no specific liability regime comparable to the scope of article 19.17 of the USMCA.[163] Mexico, nonetheless, negotiated explicit exceptions when signing the USMCA. Annex 19-A includes provisions stipulating that article 19.17 on interactive service providers does not apply to Mexico for the first three years, that some of Mexico's existing laws are deemed compliant, and that Mexico will comply in a manner that is both effective and consistent with its constitution. In addition, Parties agree that the general exceptions apply, including "measures necessary to protect public morals pursuant to paragraph (a) of article XIV of GATS".

4.3 Intellectual property (IP) protection and innovation

This section discusses provisions and exceptions in trade agreements regulating the disclosure of source code, software, and algorithms. It examines the potential implications of such provisions for regulations that aim to ensure accountability and oversight over emerging technologies such as AI, and their impact on innovation, including on policies that support technology transfer and open-software.

Overview of policy issues

The use of algorithms and automated decision-making systems is increasingly common in many areas of the economy and public life more generally, including in employment, policing and education. Despite the benefits of such systems, they give rise to relevant public policy concerns related to the risks of discrimination, including gender-based and racial-based, and lack of fairness and accountability.[164] One recent example was the controversy involving the use of algorithms to predict GCSE and A-level grades in the UK, that placed the use of machine-learning and automated decision-making systems in the public spotlight.[165] To have more transparency and understanding of the actual performance of these emerging technologies, AI ethics advocates argue that algorithms should be made visible enough to be inspected and understood, particularly when they lead to decisions that have questionable or negative consequences,[166] such as a job application denial or a driverless vehicle accident.[167] Experts have argued that, to protect individuals subject to automated decision-making, citizens should have a 'right of explanation', by which the reasoning behind a decision is presented to them.[168] There can be many ways of scrutinising an algorithm, and views on what would be the correct way vary,[169] but some forms of transparency and accountability could potentially clash with trade secrets provisions agreed in trade agreements.

As the technology landscape surrounding AI is constantly evolving, a central issue is to figure out *a priori* what type of information will be needed to police algorithms. In the context of the EU, the GDPR includes a right for individuals in certain circumstances to be informed of the logic of the systems making decisions that significantly affect them.[170] However, scholars and policymakers consider that it may be necessary to adopt further legislation or to clarify existing rules to address specific risks posed by AI systems, such as the opacity of systems based on algorithms.[171] In particular, there is a need for well-defined rights and safeguards to regulate the deployment of algorithmic decision-making tools, expanding and clarifying the scope of GDPR.[172] New rules are currently being considered. Under the proposed DSA, the European Commission would be able to order platforms to provide access and explanations relating to its databases and algorithms. The proposed legislation also establishes that very large online platforms can be audited by an independent auditor, who should have technical competence to audit algorithms and be granted access to all relevant data necessary to perform the audit properly.[173] In the UK, the government's final response to the OHWP proposed mechanisms to increase transparency from companies about their algorithm designs and to give the regulator power to request explanations about the way algorithms operate.[174] Due to the complexity and fast-evolving nature of AI and algorithms, it is not entirely clear how to equip a supervisory authority or watchdog such as the ones currently being discussed.[175]

In recent years, a number of bilateral and regional trade agreements have included IP provisions that expand the scope of protections of trade secrets to explicitly cover software and algorithms – which arguably would not be covered under the general WTO rules on trade secrets.[176] Depending on how provisions banning forced disclosure of algorithms are drafted, and the scope of their exceptions, they could potentially clash with existing proposals to improve algorithmic accountability. One the one hand, a flat-out ban on forced disclosure of source code, software and algorithm could make it harder to obtain explanations for automated decisions (including machine and deep learning) that affect individuals.[177] On the other hand, full disclosure and 'opening of the black box' might undermine IP rights and would not necessarily be required for automated systems to be accountable and to provide meaningful explanations to individuals.[178] Striking the right balance between these two policy objectives is a difficult task, in particular in light of the fast-pacing nature of emerging technologies such as AI.

Designing specific rules before one is really able to understand the underlying policy issues and the full range of exemptions that are needed is challenging. Exceptions allowing regulatory bodies and judicial authorities to access source code and algorithms, for example, can be vague and unclear regarding what type of procedures and investigations would qualify for such access to be granted. The focus on disclosure of relevant source codes to public authorities and regulatory bodies also means that, in important cases, it may not be possible to share the source code with individuals who might be affected by automated decision-making. Another challenge in drafting exceptions is that, in many cases, there are no existing legal frameworks regulating AI or transparency, so it might be difficult for

citizens to find a legal basis to argue for the disclosure of algorithms making decisions that affect their lives.

Encouraging innovation through the right balance of IP protection and support for new players is another challenge for governments. Beyond problems from the point of view of potential bias and unfairness in the decision-making that they govern, far-reaching prohibitions on disclosure of source code, software, and algorithms also have important implications for access to technology and market competition. Bans on mandatory disclosure usually seek to ensure market openness and to prevent partners from requiring the transfer of, or access to, technology as a condition for market access.[179] Such provisions aim to give firms unconditional market access for their technology-embedded products while protecting their IP, which is often a crucial element of the competitive advantage of innovative companies. These rules have gained particular relevance in light of growing concerns with governments' domestic policies requiring the disclosure of trade secrets as a condition to operate in some industries – a common policy in China.[180]

While the stated goal of these rules is to promote innovation by protecting firms' IP, provisions seeking to prohibit source code disclosure without appropriate limitations and exceptions can in fact choke access to technology that is essential to innovation, especially in less industrialised countries.[181] As source code constitutes an integral component of digital technologies, provisions prohibiting their transfer can effectively prevent the transfer of technology altogether.[182] The problem is even more acute for countries that are not fully industrialised, as strict IP rules often favour already established industries and limit developing nations' policy space to pursue legitimate regulatory objectives and development goals.[183] Indeed, in emerging economies the concept of innovation itself might differ from that of developed countries, with a greater emphasis in adopting existing technologies and 'catching up' with advanced economies rather than on creating new ones.[184] Another concern is that closing access to source code and software can stifle competition and create incentives for concentration in software markets and industry, by locking buyers into proprietary software.

Further, provisions aimed at maximising IP protection could inhibit the use or promotion of free and open-source software domestically, a relevant public policy instrument that governments should not be too hasty to relinquish. Evidence points out that open-source software is more cost-efficient and has more potential for innovation than proprietary software,[185] as it promotes spill-overs that foster the diffusion of new technologies.[186] Open-source software can also provide better security and accountability due to code transparency.[187] Moreover, the possibility of promoting the use of non-proprietary software is relevant for public procurement policies. Several countries, (developing and developed), have implemented legislation and policies that require the source code of software applications used for the provision of public services and procured by the government to be open. Some countries have domestic policies that provide preferential treatment to software packages that are open source.[188]

The UK government has been a pioneer in creating open-source software, and there is concern that trade agreement provisions could lead to challenging types of public procurement seen as preferring open source.[189] In the EU, a strategy for the internal use of open-source software was first adopted in 2000, and has since been updated three times. The most recent strategy (2020–2023) was approved by the European Commission in October 2020, and it committed to increasing even further the use of open-source software.[190] In the US, the government announced a federal source code policy in 2016, which requires that all source code be shared between agencies and mandates that at least 20% of new custom-developed source code be released as open-source software.[191] In China, open-source software is considered a tool to gain access to new technologies, and the disclosure of source code is required as a condition to ensure market access. For example, a policy from 2014 requires companies selling computer equipment to Chinese banks to disclose their source code and to submit their equipment for internal audits (Circular No. 317, Guidelines on Promoting the Application of Secure and Controllable IT, Year 2014–2015).[192]

US approach in trade agreements

The US provides extensive intellectual property protections in its recent trade agreements, and the most extensive are found in the USMCA. It explicitly includes source-code-related algorithms in the subject matter of IP protection, in addition to software protection, establishing that "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" (art. 19.16 USMCA). Provisions in the USMCA annex also ban governments from forcing companies to provide specific information about cryptography, including algorithms, as a pre-condition for market access. Exceptions are made for regulatory bodies and judicial authorities requiring access "for a specific investigation, inspection, examination, enforcement action, or judicial proceeding" so long as there are safeguards against unauthorised disclosure.

USMCA does not include balancing clauses that are found in other recent trade agreements. CPTPP text for instance introduced an 'appropriate balance' clause concerning copyright and related rights, as well as limitations and exceptions, "including those for the digital environment" (art. 18.66 CPTPP). This provision is consistent with fair use exceptions to copyright in the US and could allow for the use of copyright protected data to better train AI systems.[193]

EU approach in trade agreements

Recent agreements negotiated by the EU have included provisions banning forced disclosure of source code and software but have not gone as far as the language in US agreements to expressly include algorithms in the scope of provision.

The EU–Japan agreement did include a provision (art. 8.73) that prevents the Parties from requiring the "transfer of, or access to, source code of software owned by a person of the other Party", with exceptions laid for voluntary transfer of technology in the context of commercial contracts, government procurement, for law enforcement, and on national security grounds (general security exceptions of art. 1.5 EU–Japan). The EU–Mexico agreement includes similar provisions (art. 9, Chapter on Digital Trade), committing the Parties not to require the transfer of, or access to, source code of software owned by a company or individual from the other Party. The exceptions are also similar: for voluntary transfer in the context of a commercial contract or government procurement, investigations and law enforcement (including IP protection), or for national security or for national defence purposes. However, Article 2.a does include a broader carve-out allowing Parties to require software or source code disclosure "to achieve a legitimate public policy objective."

Similarly, in the submission to the WTO regarding e-commerce, the EU clearly states that any commitments related to consumer protection should leave "sufficient flexibility for defining the exact content and format of the relevant measures at national level" and that, with regards to prior authorisation requirements, "Members may consider relevant language reaffirming the right to regulate for legitimate public policy reasons."[194]

China's approach in trade agreements

China's poor record of protecting intellectual property has long been criticised by experts and foreign trade partners.[195] The government is also accused of 'forcing' technology transfers as a condition of doing business in the country, as it requires foreign investors to form joint ventures with Chinese firms.[196] Earlier drafts of China's Cybersecurity Law even included provisions requiring technology vendors to hand over source codes and encryption keys, although the disclosure requirement was dropped from the final version following pressure from foreign companies.[197]

Unsurprisingly, neither the China–Korea free trade agreement nor the China–Australia agreement include provisions on mandatory disclosure of source codes or algorithms. Such a provision is also absent from RCEP, but this agreement does include a provision where Parties have agreed to discuss source code as one of the emerging issues that should be considered in future dialogues on e-commerce (art. 12.16.1 RCEP).

DEPA

Different to both the US and the EU, DEPA does not contain a general clause against the mandatory disclosure of intellectual property as a condition to conduct business. It does, however, include provisions on the use of cryptography in commercial applications, establishing that Parties shall not impose or maintain regulations that require transfer of, or access to, a particular technology or information as a condition to enter the market, including in the scope of the measure cryptography

key and algorithm specification (art. 3.4 DEPA). There are exceptions in case of networks owned or controlled by the governments, including central banks; measures related to the regulation of financial institutions or markets; and law enforcement authorities, in accordance with a country's legal procedures. Importantly, DEPA includes no binding commitments to adopt AI governance frameworks, considering explainability, transparency, fairness and human-centred values (art. 8.2 DEPA).

Japan's approach in trade agreements

Japan has spearheaded proposals for the inclusion of rules in trade agreements prohibiting countries from requiring the disclosure of trade secrets, including source codes and algorithms, and banning requirements for firms to use particular encryption technologies as a condition for market access.[198] The CPTPP explicitly prohibits governments from adopting mandatory disclosure of source code or software (art. 14.17), but does not explicitly mention algorithms. Although the ban is limited to mass-market software (unless when it is used in critical infrastructure), the exceptions are narrowly defined. Governments are allowed to request disclosure in order to fulfil requests for source code modification to comply with domestic laws of regulations, in case of government procurement, and for requirements related to patent application. Provisions forbidding signatory countries from asking software companies for access to their source codes have also been proposed in the TiSA negotiations, led by Japan, Singapore, and Australia.[199]

UK approach in trade agreements

So far, the UK appears to be taking a similar approach to that of the US, negotiating relatively stringent intellectual property rules for digital technologies, but including wider exceptions, which ensures greater regulatory flexibility. In the UK–Japan agreement, the UK government has agreed to ban mandatory disclosure of source code, software and algorithms expressed in that software (art. 8.73 UK–Japan). Previous EU agreements, including the one with Japan, already included prohibitions on forced disclosure of source code and software, but the UK–Japan agreement innovated by expanding the scope of the protection to include "algorithms expressed in that source code." The wording in the UK–Japan provision on source code is, in fact, very similar to the analogue articles in the USMCA (art. 19.16), as discussed above.

Even though the scope of the UK–Japan prohibition is similar to the language found in the USMCA, the exceptions are more similar to the ones found in EU agreements and provide greater flexibility for government policymaking. While the exceptions in US agreements are restricted to allowing regulatory bodies and judicial authorities access for a specific procedure, the UK–Japan agreement, (as for the EU–Japan agreement), includes exceptions to allow regulatory or judicial bodies to access source codes and algorithms, which can also be requested to protect national

security, integrity of the financial system, and for a series of public policy objectives listed in the general exceptions (art. 8.3 UK–Japan).

The UK–Japan agreement also includes a novel provision banning the Parties from requiring access to cryptography technology. The provision bans measures that require companies to transfer or provide access to any proprietary information relating to cryptography, including the disclosure of a private key or algorithm specification (art. 8.86 UK–Japan). As cryptography is often a privacy-enhancing tool, this could be in the benefit of consumers, but it is unclear what the UK government rationale was in adopting this specific provision. A similar provision on cryptography was included in the recent Digital Economy Partnership Agreement between New Zealand, Singapore and Chile (art. 3.4 DEPA).

The UK–EU TCA includes binding commitments against the forced transfer of source code of software (art. DIGIT.12), but, in contrast to the UK–Japan agreement, it does not explicitly mention algorithms. As with previous EU agreements, this provision is subject to general exceptions, security exceptions, and prudential carve-out (Article DIGIT.4), and the ban does not apply to disclosure requests made by a court or administrative tribunal, nor by regulatory bodies.

The US is likely to place demands on the UK to introduce strong intellectual property rules in the negotiated trade agreement.[200] The US clearly states among its negotiation objectives the aim to establish "rules to prevent governments from mandating the disclosure of computer source code or algorithms."[201] As discussed above, the inclusion of such a provision has been consistent in previous trade agreements celebrated by the US (eg the USMCA).

So far, the UK approach with regards to disclosure of source code, software, and algorithms is located mid-way between that of the US and of the EU. While the scope of the UK provisions is similar to those in recent US agreements, seeking broader and more stringent IP protections, the exceptions are closer to those found in EU agreements, providing greater regulatory autonomy.

4.4 E-commerce – trade facilitation and consumer protection

This section examines the rules and regulations in trade agreements that aim to facilitate e-commerce and protect consumers engaging in e-commerce transactions.

Overview of policy issues

E-commerce refers to the production, distribution, marketing, sale or delivery of goods and services by electronic means. As the economy has digitalised, business-to-business (B2B) and business-to-customer (B2C) transactions have increasingly moved online, a trend intensified by the COVID-19 pandemic.[202] An increasing amount of trade is conducted digitally: as at 2018, UNCTAD estimated that the global value of e-commerce sales (B2B and B2C) reached almost US$26 trillion, equivalent to 30% of global GDP.[203] Globally the US dominates the e-commerce

market accounting for one-third of global e-commerce sales in 2018, followed by Japan, China, Korea and the UK. As at 2018, the largest e-commerce companies were based in the US and China: the US is home to five of the largest ten B2C e-commence companies; China is home to four; and Japan to one.[204]

The growth in e-commerce has generated demand for governments to create new rules and regulations to facilitate cross-border e-commerce and to ensure that businesses and consumers are protected, including from fraudulent, misleading or deceptive conduct.

Paper-based documents have been used to support commercial transactions for centuries, whether in a national or a cross-border context. Moving these processes online creates new challenges. In the digital environment, Parties need to find ways to ensure that the people signing documents are who they say they are, without necessarily seeing them in person, or, that the transaction document in question has not been tampered with, copied or otherwise changed. Parties also need to have confidence that their information will not be misappropriated or details copied. Rules and regulations also have to keep up with the numerous and rapidly changing technologies and methods for electronically exchanging contractual information and authenticating documents.[205]

[206]At present, there is no universal system of standards, technologies or regulations for e-transactions, and governments have introduced different types of e-transaction laws. For instance, in the area of e-signatures, some countries (including US, Canada, Australia, New Zealand and Singapore) take a minimalist approach and accept all forms of electronic or digital signatures, leaving it up to the Parties to a transaction to agree on the form. A few governments, including Indonesia, take a completely prescriptive approach, requiring Parties to employ a specific government-authorised method or technology when signing documents electronically. Others, (including the EU, Brazil, Chile, China, India, Mexico and South Africa), adopt hybrid approaches. In the EU, for instance, all types of signature are legal, admissible, and enforceable, but only e-signatures that meet specific criteria are legally identical to handwritten signatures.[207]

Divergent domestic rules on e-transactions, e-signatures and authentication make cross-border digital activities more complex and raise the cost of doing business in multiple markets. Differences between legal frameworks can also lower confidence in e-commerce, since consumers may be uncertain of the relevant legal norm or standard. This is compounded by a lack of transparency in many countries on the grounds of an e-signature's acceptability for cross-border trade.[208]

Since the 1990s, the United Nations Commission on International Trade Law (UNCITRAL) has developed a series of model laws to guide states in drafting legislation on e-commerce (1996), e-signatures (2001), and electronic transferable records (2017). There are three core principles advanced by these model laws. First, non-discrimination between paper-based and electronic forms of communication. Second, technological neutrality, such that laws do not insist on a specific technology for recognising the validity of electronic transactions. Third, functional equivalence, setting out which electronic communications may be considered

equivalent to paper-based notions such as 'writing', 'original', 'signed', and 'record'.

As UNCITRAL model laws are non-binding, governments have increasingly turned to trade agreements to promote paperless trading and the use and harmonisation of rules on e-signatures, digital signatures, e-authentications, and digital identities.[209] Provisions on e-commerce are the most common form of digital trade provision in bilateral and regional trade agreements, and they are also being negotiated in ongoing WTO negotiations on e-commerce.[210]

There have been some efforts to include provisions that protect consumers engaging in international e-commerce transactions and provide them with mechanisms for redress, but these have received less attention, perhaps reflecting the limited advocacy and lobbying resources of consumer groups compared with business organisations. Consumers in many countries are wary of engaging in online transactions, (particularly cross-border), out of concern that transactions and delivery are less secure, and remedies do not exist when something goes wrong. Online consumer protection rules have the potential to regulate the 'pre-purchase' stage (including advertising, information requirements, unfair commercial practices, etc.), the 'purchase' stage (including unfair contract terms, online payment security, etc.) and the 'post-purchase' stage (including dispute resolution, redress requirements, etc.). While many countries have consumer protection laws for online transactions, regulatory approaches vary. Some governments rely on industry self-regulation and market supervision by consumer associations, while others regulate more explicitly, adopting laws and regulations that provide e-consumers with rights regarding the return and cancellation of goods and services, and relating to the protection of data privacy.[211]

At international level, the UN and OECD actively promote online consumer protection through soft law guidance. The UN General Assembly adopted the Guidelines for Consumer Protection in 1995 (revised in 1999 and 2015) which aim at ensuring a minimum level of consumer protection, including online. Since 1999 the OECD has also promulgated guidance on consumer protection in e-commerce, updating its guidance to reflect evolving digital technologies. In 2018 the G20/OECD agreed a statement of Policy Guidance on Financial Consumer Protection Approaches in the Digital Age. So far, provisions in trade agreements on consumer protection in e-commerce have been weak and fall short of imposing mandatory obligations. Discussions at the WTO on e-commerce include discussions on consumer protection, but they are vague about the substantive content. Many bilateral and regional agreements contain provisions but few include binding substantive commitments.[212]

US approach in trade agreements

The US positions on e-commerce are reflected in the recent texts of USMCA, US Japan, and US proposals at the WTO.[213] They include commitments to paperless trading, with each Party endeavouring to accept a trade administration document submitted electronically as the legal equivalent of the paper version of that

document (eg art. 19.9 USMCA), and committing to maintain a domestic legal framework consistent with the UNICTRAL Model Law on Electronic Commerce (1996) (eg USMCA art. 19.5).

There are also provisions on e-authentication and e-signatures where Parties commit to uphold non-discrimination between paper-based and digital versions; to not prohibit Parties to a transaction from mutually determining the appropriate authentication methods or e-signatures, subject to an exception that allows a Party to require e-signatures and methods of authentication to meet certain performance standards or attain certification, for specific types of transactions; and to promote interoperability (eg USMCA art. 19.6). The US approach then rules out wholly prescriptive approaches to e-signatures and e-authentication, but accepts both minimalist and hybrid approaches.

Provisions on consumer protection include commitments to "adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers" but no details are given as to the nature of these measures (eg art. 19.7 USMCA). There are measures on spam, with Parties agreeing to adopt or maintain measures providing for the limitation of "unsolicited commercial electronic communications" but the content of these measures is weak, with Parties only agreeing to require suppliers to *facilitate the ability* of recipients to prevent ongoing reception of those messages *or* require the consent of recipients (eg art. 19.13 USMCA).

EU approach in trade agreements

The EU takes an approach to digital trade facilitation that is very similar to that in the US. In the EU–Japan text and the EU's proposal in WTO e-commerce negotiations, the provisions on e-authentication and e-signatures are very similar to those in the USMCA (eg art. 8.77 EU–Japan).[214] EU agreements also have additional specific provisions on the conclusion of contracts by digital means, with Parties agreeing not to use measures that deny the legal effect, validity or enforceability of a contract, solely on the grounds that it is concluded by electronic means (eg art. 8.76 EU–Japan).

The EU, like the US, has not championed strong consumer protection measures. Provisions on consumer protection in EU–Japan stop short of making commitments to uphold or maintain consumer protection laws, noting simply that they are important and committing to co-operation (art. 8.78 EU–Japan), although the EU's proposal at the WTO does propose that Parties commit to measures that protect consumers from fraudulent and deceptive commercial practices. The one area that the EU provisions are slightly stronger is on spam, where EU agreements typically require the prior consent of recipients to receive commercial electronic messages (eg art. 8.79 EU–Japan). More recent EU proposals, including for negotiations with Australia (art. 12 Digital Trade proposal, dated 2018) are stronger as they stipulate in greater detail how consumers are to be protected.[215]

China's approach in trade agreements

E-commerce is one of the areas that China has been keen to include in its recent trade agreements, including with Korea (2015) and Australia (2017). The RCEP chapter (2020) on e-commerce provides a more recent insight into the China's positions. In this section and all discussions that follow, it is important to remember that provisions on e-commerce in the China–Korea, China–Australia, and RCEP are not subject to the dispute settlement chapter (art. 13.9 China–Korea; art. 12.11 China–Australia; art. 12.17 RCEP) and, as such, are subject only to 'good faith' consultations.

On paperless trading, China has committed to "accept the electronic versions of trade administration documents as the legal equivalent of paper documents" with some exceptions, to "endeavour" to take into account the methods agreed by international organisations, and to make all trade administration documents available to the public as electronic versions (art. 12.9 China–Australia). China has also committed to maintaining domestic legal frameworks governing electronic transactions based on the UNCITRAL Model Law on Electronic Commerce 1996 and other relevant international standards (art. 12.5 China–Australia). The provisions are weaker in RCEP, where Parties will "work towards" paperless trading with least developed countries having five years' grace to comply, and "endeavour" to accept electronic trade administration documents as equivalent (art. 12.15 RCEP). Parties commit to a domestic legal framework that "takes into account" the relevant UNCITRAL, UN, or other international conventions and model laws on e-commerce and "endeavour" to avoid "any unnecessary regulatory burden on electronic transactions" (art. 12.10 RCEP).

With regards to e-authentication and e-signatures, China has, like the US and EU, agreed to non-discrimination provisions that allow minimalist and hybrid approaches but rule out completely prescriptive approaches. The China–Korea FTA commits to non-discrimination, allowing private parties to transactions to decide what authentication technologies they want to use (art. 13.4 China–Korea). While Korea stipulates that it may require that the method of authentication meets certain performance standards or be certified, China does not make this stipulation (footnote to art. 13.4 China–Korea). Parties also agree to work towards mutual recognition of digital certificates and e-signatures (art. 13.4 China–Korea; art 12.5 China–Australia). The wording in RCEP is similar to the US and EU and allows greater regulatory discretion: while Parties agree that a legal signature cannot be rejected solely because it is in electronic form, although there is an exception that allows for the use of performance standards and certification requirements for certain categories of transactions (art. 12.6 RCEP).

As in US and EU agreements, China's commitments on consumer protection in its trade agreements are weak, as "Each Party shall, to the extent possible and in a manner it considers appropriate, provide protection for consumers using e-commerce that is at least equivalent to that provided for consumers of other forms of commerce under their respective laws, regulations and policies" (art. 12.7 China–Australia). RCEP similarly requires Parties to have measures that provide "protection for consumers using e-commerce against fraudulent and misleading practices that cause harm or potential harm to such consumers" without setting any minimum

standards, and with a five-year grace period for least-developed countries (art. 12.7 RCEP). With regards to spam, there are no provisions in the China–Korea or China–Australia agreements, and there are commitments in RCEP where Parties must adopt measures. However, as in US agreements, prior consent is not required, and measures may be limited to particular modes of delivery, such as email, rather than the more lucrative forms, such as unsolicited advertising or targeted messaging (art. 12.9 RCEP).[216]

DEPA

The most ambitious e-commerce provisions are found in the DEPA, between New Zealand, Singapore, and Chile. The text includes stronger commitments on paperless trading, with Parties committing to make all existing publicly available trade administration documents public in machine-readable electronic formats; to accept electronic versions of trade administration documents as the legal equivalent of paper documents, subject to limited exceptions; to establish or maintain a "seamless, trusted, high-availability and secure interconnection" between their respective single windows to facilitate the exchange of data relating to trade administration documents; and to promote systems for the exchange of electronic records used in commercial trading activities between the Parties' businesses (art. 2.2 DEPA).

On e-authentication and e-signatures, the DEPA Parties make similar commitments to that of the USMCA text, committing to maintain a domestic legal framework consistent with the UNICTRAL Model Law on Electronic Commerce (1996) or the United Nations Convention on the Use of Electronic Communications in International Contracts (2005). But they go further in stating that they will also endeavour to adopt the UNCITRAL Model Law on Electronic Transferable Records (2017) (art. 2.3 DEPA).

On consumer protection, DEPA provisions are also more extensive than those found in recent agreements of the US, EU, and China. While Parties similarly agree to "adopt or maintain laws or regulations to proscribe fraudulent, misleading or deceptive conduct" DEPA goes further in specifying in detail what "fraudulent, misleading or deceptive conduct" includes. In addition, Parties agree to adopt or maintain laws or regulations that require goods and services provided to be of acceptable and satisfactory quality, consistent with the supplier's claims regarding the quality of the goods and services; and provide consumers with appropriate redress when they are not (art. 6.3 DEPA). Provisions on spam are similar to those found in recent EU agreements, as measures used to address spam must require consent of recipients to receive commercial electronic messages (art. 6.2 DEPA).

The DEPA text also includes new commitments to share best practices on cross-border logistics (art. 2.4 DEPA); to work together to promote the adoption of e-invoicing by businesses, and base any measures related to e-invoicing on international standards, guidelines or recommendations in order to support cross-border interoperability (art. 2.5 DEPA); and implement expedited customs procedures for express shipments and provide for a *de minimis* shipment value or dutiable amount for which customs duties will not be collected (art. 2.6 DEPA). There

is a provision on electronic payments, with Parties committing to support the development of efficient, safe, and secure cross-border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability and the interlinking of payment infrastructures, and encouraging useful innovation and competition in the payments ecosystem (art. 2.7 DEPA).

UK approach in trade agreements

The area of e-commerce is unlikely to be a contentious one in the UK's upcoming trade negotiations. The main question is how ambitious the UK wants to be in terms of the coverage of e-commerce provisions and strength of consumer protection provisions. So far, the UK has not been particularly ambitious, and has opted to simply follow the EU's fairly minimalist approach.

The TCA between the UK and the EU includes binding commitments to ensure that contracts may be made by electronic means and have equivalent effect, subject to exceptions for some types of contract (art. DIGIT.10 TCA). The UK–Japan agreement simply replicates the provision in the EU–Japan agreement which is more simply worded and allows for greater regulatory flexibility. Instead of listing specific exceptions, the commitment is qualified with the phrase "Unless otherwise provided for in its laws and regulations" (art. 8.76 UK–Japan).

The TCA includes an article on e-authentication and electronic trust services. While similar to articles in recent US and EU trade agreements, it covers a more expansive list of electronic forms of authentication: "A Party shall not deny the legal effect and admissibility as evidence in legal proceedings of an electronic document, an e-signature, an electronic seal or an electronic time stamp, or of data sent and received using an electronic registered delivery service, solely on the ground that it is in electronic form" (art. DIGIT.11 TCA). It also stipulates more restrictions on the measures that governments can impose as such requirements: "shall be objective, transparent and non-discriminatory and shall relate only to the specific characteristics of the category of transactions concerned" (art. DIGIT.11 TCA). This qualification is similar to that found in the EU–Mexico agreement and EU proposals at the WTO.[217] The new UK–Japan agreement replicates the EU–Japan text (which is narrower as it only applies to e-signatures or authenticating data resulting from e-authentication). However, it goes beyond the EU–Japan text by incorporating the more restrictive language regarding the exception for government regulations (art. 8.77 UK–Japan). Neither the TCA nor the UK–Japan agreement contain commitments on paperless trading, cross-border logistics, expedited customs procedures and *de minimis* thresholds, electronic payments, or e-invoicing, which are found in the DEPA and which UK technology companies have called for.[218]

With regards to online consumer protection, the UK has not advocated a robust approach to date. In the TCA, the UK proposed weaker language than the EU, and the final text largely reflects the EU proposals. The TCA stipulates in detail the nature of the consumer protection measures that the Parties will adopt. These include measures that "proscribe fraudulent and deceptive commercial practices"; "require suppliers of goods and services to act in good faith and abide by fair commercial

practices, including through the prohibition of charging consumers for unsolicited goods and services"; "require suppliers of goods or services to provide consumers with clear and thorough information"; and "grant consumers access to redress for breaches of their rights, including a right to remedies if goods or services are paid for and are not delivered or provided as agreed" (art. DIGIT.13 TCA). The Parties also "recognise the importance of entrusting their consumer protection agencies or other relevant bodies with adequate enforcement powers" and the importance of co-operation between these agencies to protect consumers and enhance online consumer trust (art. DIGIT.13 TCA). These provisions are stronger than in the UK–Japan agreement, which simply replicated the minimalist approach of the EU–Japan agreement (art. 8.79 UK–Japan).

Similarly, on spam, the TCA reflects EU proposals, placing emphasis on obtaining the consent of users as "Each Party shall ensure that direct marketing communications are not sent to users who are natural persons *unless they have given their consent* in accordance with each Party's laws to receiving such communications" (art. DIGIT.14 TCA, emphasis added). An exception is made where the supplier has already collected, in accordance with conditions laid down in the law of that Party, the contact details of a user in the context of the supply of goods or service, in which case the supplier can send direct marketing communications to that user for their own similar goods or services. This is stronger than the provision in the UK–Japan agreement, where the requirement of prior consent was dropped, and the text follows the US approach (art. 8.81 UK–Japan).

4.5 Customs duties and digital services taxes

This section examines how trade agreements might limit states' freedom to impose digital sales taxes and customs duties, as well as the different positions adopted by key states on the topic.

Overview of policy issues

As the digital economy has grown, there is increasing financial and public pressure on governments to change tax regimes, as many larger digital economy companies have paid low levels of tax despite high levels of profits, due to their non-resident status. There are major international initiatives underway to discuss how best to adjust tax regulations to the realities of the digital economy, led by the OECD and G20 countries. The issue for trade policymakers is whether, and to what extent, the trade regime and commitments under international trade agreements constrain the ability of governments to effectively tax the digital economy. There are two specific areas where there is a live and ongoing debate: customs duties on e-commerce, and the use of digital services taxes.

In 1998, as the digital economy was beginning to take off, WTO Members agreed to a two-year moratorium on customs duties on electronic transmissions (WTO Moratorium), with a view to encouraging this new aspect of global trade.[219] Since then, at every Ministerial Conference, WTO Members have agreed to "maintain the current practice of not imposing customs duties on electronic transmissions".[220]

However, the definition of the term 'electronic transmissions' has never been agreed and is disputed, so the scope of this obligation remains unclear.[221] While there is general agreement that the WTO Moratorium applies to customs duties (not domestic and internal taxes) and to digitally delivered products, there are major disagreements on coverage and on whether it should be made permanent.

Disagreements on customs duties on digital trade are split along North–South lines. Many industrialised countries strongly advocate for coverage of both goods and services and for the WTO Moratorium to be made permanent, arguing that this benefits consumers and would enhance digital trade flows.[222] In contrast, a number of developing countries, most notably India and South Africa, are strongly opposed, arguing that it is "equivalent to developing countries giving the digitally advanced countries duty-free access to [their] markets",[223] leads to substantial revenue losses and undermines digital economy industrial policy.[224] As discussed in more detail below, in addition to ongoing discussions at the WTO, the US, EU, and several other countries have included provisions in their free trade agreements that prohibit the imposition of customs duties on digital products transmitted electronically.

Digital services taxes are similarly contentious, although the tensions are largely between the US and other jurisdictions, including the EU. In the past few years, governments have started to introduce taxes on the provision of digital services, including Austria, Brazil, Czech Republic, France, India, Indonesia, Italy, Spain, Turkey, and the UK.[225] The EU has been preparing a proposal for an EU-wide digital tax, to avoid the fragmentation of the single market.[226] The rationale for these taxes is that internet platforms should pay tax where they are located, and also where they make their profits (that is, where their users reside).[227] The US, which is home to many of the world's largest digital services companies, has strongly opposed the introduction of digital services taxes. In 2019, the US launched an investigation into France's digital services tax, and found that the tax was discriminatory and inconsistent with prevailing international tax principles. The US threatened to impose retaliatory tariffs, which caused France to temporarily suspend its planned tax.[228] As of January 2021, France had resumed collecting the tax and the US had decided to defer the imposition of tariffs on French goods as a response.[229]

There is an increasing discussion in the trade policy world about the compatibility of digital services taxes and the commitments that governments have made in trade agreements. The discussion is complex and disputed: it largely depends on how the digital services tax is designed, and is not aided by the fact that experts disagree on whether a digital services tax is a form of tariff,[230] transaction tax,[231] an income tax,[232] or something akin to an excise tax.[233] With regards to WTO rules, most experts agree that the WTO Moratorium does not affect the use of digital services taxes as they are not custom duties and fall out of its scope.[234] Obligations under GATS are more likely to have implications for digital services taxes. GATS came into force in 1995, before the growth of the digital economy. Although the agreement is technologically neutral (that is, commitments apply irrespective of how the services are delivered), there is no consensus as to whether digital services that did not exist at the time of adoption (such as cloud storage or music streaming) are covered by existing commitments.[235]

Insofar as GATS commitments do apply to digital services, the way some digital services taxes are drafted, or their practical effects, could put them at odds with non-discrimination commitments (national treatment (art. XVII GATS) and most-favoured nation treatment (art. II GATS)).[236] The main concern is with national treatment obligations as GATS prohibits less favourable treatment of 'like' services and service suppliers for sectors listed in a Member's Schedule of Commitments, subject to express limitations. For national treatment purposes, likeness "depends in principle on attributes of the product or supplier per se rather than on the means by which the product is delivered" – meaning that the mere fact that a service is delivered digitally does not make it unlike its non-digital equivalent. Thus, for instance, by targeting only the digital sector, digital services taxes might discriminate between online and offline versions of 'like' services and service suppliers and hence contravene national treatment obligations. For example, app-based private car hiring services (such as Uber) might be subject to the tax, but not telephone-based private car hiring services.[237] It is less likely that digital services taxes contravene most-favoured nation obligations under GATS. This could happen if the thresholds of a digital services tax generate a *de facto* discrimination against companies from one foreign state in comparison to companies from another foreign state, but this does not seem likely under the digital services taxes introduced to date.

Under GATS there are exceptions to non-discrimination obligations, but the tax carve-outs are generally not applicable to digital services taxes[238] and it is unclear whether the general exceptions under GATS XIV would apply. However, 19 countries (including the US but excluding the EU, China, Australia, and New Zealand) have scheduled broad horizontal exceptions on tax in their GATS services schedules and, depending on how these are drafted, may cover digital services taxes.[239]

Even if a digital services tax is consistent with a state's WTO commitments, it may be challenged under a bilateral or regional trade agreement. Bilateral and regional trade agreements often make services commitments that extend beyond their GATS commitments, widening the applicability of non-discrimination obligations. So far agreements have not included specific reference to digital services taxes. Whether or not a digital services tax is likely to breach commitments depends on the design of the tax as well as the specific drafting of non-discrimination provisions in the services and digital trade chapters, as well as the nature of general exceptions, particularly those on tax. Few bilateral and regional trade agreements regulate digital services taxes more strictly than the GATS, and some agreements have far more extensive tax carve-outs.[240]

US approach in trade agreements

The US is a strong advocate for making the WTO Moratorium permanent. Many US bilateral and regional agreements have clauses prohibiting the imposition of customs duties on digital products transmitted electronically. For instance, the USMCA states that "No Party shall impose customs duties, fees, or other charges on or in connection with the importation or exportation of digital products transmitted

electronically, between a person of one Party and a person of another Party" (art. 19.3 USMCA).

With regards to digital services taxes, while there are no explicit provisions that restrict the use of digital services taxes, questions have been raised about the compatibility of digital services taxes with the commitments on cross-border data flows that are found in recent US agreements. Commentators have pointed that, should a digital services tax amount to a 'restriction on cross-border data flows', then it could be incompatible, depending on whether 'the tax design is discriminatory or [has] protectionist purposes".[241] Perhaps unsurprisingly, unlike other jurisdictions, the US has not sought to strengthen the tax exception in its trade agreements. Under the USMCA and US–Japan agreement or instance, a digital services tax is no more likely to be covered by a tax exception than under GATS.[242]

Rather than try and negotiate provisions in trade agreements that explicitly restrict the use of digital services taxes, the US has opted to use unilateral trade measures. In June 2020, the United States Trade Representative (USTR) launched an investigation on a series of existing and proposed digital services taxes in Austria, Brazil, the Czech Republic, the EU, India, Indonesia, Italy, Spain, Turkey, and the UK. The investigation sought to determine whether an act, policy, or practice of a foreign country is actionable under section 301 of the US Trade Act 1974. Actionable matters include "inter alia, acts, polices, and practices of a foreign country that are unreasonable or discriminatory and burden or restrict U.S. commerce". A practice is deemed unreasonable "if the act, policy, or practice, *while not necessarily in violation of, or inconsistent with, the international legal rights of the United States*, is otherwise unfair and inequitable" (emphasis added). Thus, under section 301, the foreign country does not need to be in contravention of international commitments in order for actions to be taken.

In early 2021, the USTR issued the first reports of its investigations, finding that digital services taxes in Austria, Italy, India, Spain, Turkey, and the UK discriminated against US companies, were inconsistent with international tax principles, and were a burden or restricted US commerce.[243] The USTR decided against the immediate imposition of tariffs, leaving the decision on how to address the digital services taxes of the UK and other states to the incoming Biden administration.[244]

EU approach in trade agreements

The EU, like the US, is seeking to make the WTO Moratorium permanent and EU agreements similarly prohibit the imposition of customs duties on electronic transmissions (eg art. 8.72 EU–Japan; art. 3 EU–Mexico chapter on digital services). This position is also reflected in the EU proposals at the WTO.[245] The EU has sought to explicitly include services in its definition of electronic transmissions. In its WTO position, it proposes that electronic transmissions should include 'transmitted content', and in its proposals in ongoing negotiations, including with Australia, it is even more explicit that "Electronic transmissions shall be considered as a supply of

services within the meaning of the Title on Investment Liberalisation and Trade in Services".[246]

Unlike the US, the EU is supportive of digital services taxes, and a challenge for the EU is to design these taxes in ways that are in line with its international trade obligations. The OECD has issued a number of reports on the tax challenges arising from digitalisation, aimed at providing "a solid foundation for a future agreement" based on net taxation of income and avoidance of double taxation.[247] In some recent trade agreements, the EU has strengthened the general exceptions on taxes (eg art. 28.7 CETA) which appears to exempt digital services from non-discrimination obligations.[248]

China's approach in trade agreements

China has sided with India and South Africa in discussions on the WTO Moratorium,[249] and has refrained from making any commitments in its trade agreements that prohibit the imposition of customs duties. In the China–Korea agreement, for instance, the Parties agreed instead to "maintain the current WTO practice of not imposing customs duties on electronic transmissions" but the commitment is "made without prejudice to the Parties" position on whether deliveries by electronic means should be categorised as trade in services or goods (art. 13.3 China–Korea FTA). Similar provisions are found in the China–Australia FTA (art. 12.3), and RCEP (art. 12.11 of RCEP).

China does not impose digital services taxes. However, in line with a wider shift in Chinese policy towards more stringent regulation of large digital companies, the government has been considering the use of digital services taxes on platform companies. In contrast to digital services taxes introduced by other countries, in China's case the target would be large domestic platform companies.[250] Like the EU, some moves have been made to exclude digital services taxes from the scope of the agreement, with the China–Australia FTA providing more expansive exception for tax measures than that found in GATS.[251]

DEPA

On customs duties, DEPA includes a provision that prohibits customs duties on "on electronic transmissions, including content transmitted electronically" (art. 3.2 DEPA). With regards to digital services taxes, DEPA contains one of the strongest stand-alone carve-outs on taxation of any trade agreement, providing an almost total exception for tax measures (art. 15.5 DEPA).

UK approach in trade agreements

The UK's approach on customs duties on e-commerce is strongly aligned with that of the EU and US. The UK has declared itself a strong supporter of the WTO Moratorium and is calling for it to be made permanent.[252] The UK–Japan agreement contains a commitment not to impose customs duties, and it is more specific than the one found in the earlier EU–Japan agreement as it specifies that the prohibition includes

"content transmitted digitally" and specifies that the prohibition "does not apply to internal taxes, charges and other fees unless they are imposed in a manner inconsistent with the Agreement" (art. 8.72 UK–Japan). The EU–UK TCA clearly stipulates that "electronic transmissions shall be considered as the supply of a service" and that the Parties "shall not impose customs duties on electronic transmissions" (art. DIGIT.8). The UK and US negotiating objectives both specify that any UK–US trade agreement should contain a similar prohibition.

Digital services taxes are likely to be a more contentious issue for the UK, particularly in the context of trade negotiations with the US, as some US senators have warned that the UK's digital sales tax could derail trade negotiations.[253] The UK introduced a digital services tax in April 2020, a tax of 2% on revenues made by large platforms that service UK-based users. It applies to businesses that provide a social media platform, search engine, or online marketplace services, which have global revenues of more than £500 million a year and UK revenues of more than £25 million a year.[254] In January 2021, the USTR reported that the UK's digital services tax was inconsistent with the principles of international taxation, though it made no mention of inconsistency with obligations under international trade agreements.[255]

Some analysts argue that the UK's digital services tax is likely to contravene its GATS obligations on non-discrimination.[256] Specifically, the 'low profit' threshold for exemption might be incompatible with GATS national treatment obligations. Some commentators have pointed that "[if] the exemption is based on low profits as calculated by UK tax rules, then firms that are not subject to the UK corporate income tax (because they do not have a permanent establishment in the UK) will not be eligible for the exemption".[257] In other words, UK-based companies would have a more favourable treatment than foreign-based companies. Similarly, as the UK Digital Services Tax (DST) only applies to companies of a certain economic size, it could be *de facto* discriminatory if all or most of the companies subject to it were foreign-based,[258] something that is still unclear.

As the UK negotiates free trade agreements with other countries, and looks to accede to the CPTPP, care will need to be taken to ensure that the commitments it makes are compatible with the design of its digital services tax. The UK might consider including stronger tax exceptions. For instance, the general exception for tax measures in the UK–Japan agreement replicates the provision in the EU–Japan agreement, which is less extensive than the tax carve-outs in DEPA and CETA.

5. Conclusion

The UK government has rightly identified digital trade as an important aspect of its trade agenda. Digital technologies are evolving rapidly, and policymakers around the world are working out how best to regulate the digital economy nationally and internationally, to harness the opportunities it presents and mitigate the risks it poses. As we have explained, the regulation of the digital economy is a contentious area of international policy, with the US, the EU, and China taking very different approaches in many areas. As the UK steps back from membership of the EU, it will

need to identify its policy priorities, and to craft a digital trade strategy that navigates effectively between the approaches of these major digital realms.

As this paper has shown, how the UK approaches the negotiation of digital trade chapters in free trade agreements and at the WTO will have a wide range of public policy implications. In developing a digital trade strategy, decisions will need to be made about how best to support businesses and workers across the UK to benefit from the digital economy, including by promoting innovation and competitive markets and the creation of high-quality jobs; to ensure that consumers can trust the online environment; to protect the privacy and uphold the digital rights of citizens; to ensure the accountability and transparency of new technologies; and to fairly tax the digital economy.

The UK will need to be alert to emerging issues too. Beyond the issues covered in this paper, trade policymakers are increasingly concerned about how to reconcile cybersecurity measures with international trade rules. As digital connectivity grows, so does the risk of cyberattacks, and in the context of increasing geostrategic rivalry between major powers, governments are taking cybersecurity measures that restrict trade and investment. These include data-localisation requirements and import and investment restrictions on data and information technology products, particularly from countries or along supply chains where cyber risk is high. Import restrictions, including higher tariffs, are also being used to punish and deter cyberattacks.[259] Although trade agreements have security exceptions that can be invoked to justify such measures, these were not drafted with cybersecurity in mind, and the trading system will need to find ways to distinguish legitimate cybersecurity measures from unjustified protectionism.[260] Addressing the interface between cybersecurity and international trade rules will be a major issue for trade policymakers, and the UK will need to carefully align its trade policy with its foreign and defence policies.[261]

The UK's international development policies will also come into play. At a global level there are important decisions to be made over how to regulate the global digital economy to ensure that the gains from digitalisation are more evenly distributed across the world. The rules agreed in international trade agreements at the bilateral and multilateral level will have implications for access to and control over new digital technologies, and the taxation of digital economy, and there are emerging tensions between industrialised and developing countries. This is an area where the UK could work to ensure that global negotiations over digital trade are more inclusive and prioritise the interests of developing countries, particularly low-income developing countries.

The analysis in this paper highlights the need for a carefully crafted, robust, and evidence-based approach to digital trade, which looks beyond a narrow approach of maximising short-term economic gains. In each area of digital trade, the UK government will need to appraise the available policy options, and work to understand their implications for businesses, workers, consumers, and the digital rights of citizens. Internationally, the UK has important decisions to make about how it will navigate between the US, EU, and Chinese approaches to digital economy

regulation, and how it will work to ensure that the emerging international rules support the attainment of the UN Sustainable Development Goals.

To be effective, the UK's digital trade strategy will need to be integrated with other policy areas, including industrial, innovation and employment policies, competition policy, consumer protection policy, and its taxation policy. It will need to be formulated through close cross-Whitehall co-ordination including with the Department for Digital, Culture, Media & Sport, the Department for Business, Energy & Industrial Strategy, and the Information Commissioner's Office.

Precisely because digital trade is a contentious area of policy, it is important to have high-quality information in the public domain, thorough consultation with a wide range of stakeholders, and effective parliamentary scrutiny. In all these areas there is room for improvement. To date, the quality and extent of publicly available evidence and analysis on digital trade has been limited, there is very little informed public debate, and government has yet to set out a detailed strategy for digital trade.[262] The government has established a trade advisory group on telecoms and technology, but only businesses are represented, providing consumer groups, trade unions, and policy experts with limited opportunities for meaningful input.[263] Parliament has few scrutiny powers committees charged with scrutinising trade agreements, and they have insufficient time to perform this role effectively.[264] Improving the quality of information, consultation, and parliamentary scrutiny of digital trade would help to ensure high-quality decision-making and secure public confidence.

---

[1] UK Government, *DCMS Economic Estimates 2019 (Provisional): Gross Value Added*, 10 December 2020, Department for Digital, Culture, Media & Sports, available at https://www.gov.uk/government/publications/dcms-economic-estimates-2019-gross-value-added/dcms-economic-estimates-2019-provisional-gross-value-added (accessed 5 February 2021] *DCMS Sector Economic Estimates: Employment Oct 2019 - Sep 2020*, 21 January 2021, Department for Digital, Culture, Media & Sports, available at https://www.gov.uk/government/statistics/dcms-sector-economic-estimates-employment-oct-2019-sep-2020 (accessed 5 February 2021).

[2] M. Lee et al., *Understanding and Measuring Cross-Border Digital Trade - Final Research Report* (2020) 93, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf. (accessed 17 February 2021).

[3] Department for International Trade and E. Truss, *Liz Truss Launches Future Trade Strategy for UK Tech Industry*, 9 June 2020, GOV.UK, available at https://www.gov.uk/government/news/liz-truss-launches-future-trade-strategy-for-uk-tech-industry (accessed 26 October 2020).

[4] E. Jones and B. Kira, *The Digital Trade Provisions in the New UK-Japan Trade Agreement: Submission to the International Trade Committee*, UK House of Commons, 7 November 2020, available at https://committees.parliament.uk/writtenevidence/14812/html/ (accessed 18 January 2021).

[5] techUK, *Data, Adequacy and the Future Relationship – an Explainer*, 28 December 2020, available at https://www.techuk.org/resource/data-adequacy-and-the-future-relationship-an-explainer.html (accessed 18 January 2021.

[6] K. Schwab, 'The Fourth Industrial Revolution', (2016), available at https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution (accessed 18 January 2021).

[7] WTO, *World Trade Report 2020: Government Policies to Promote Innovation in the Digital Age* (2020) 208, available at https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20_e.pdf (accessed 18 January 2021).

[8] M. Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, RTA Exchange Overview Paper (2017), available at https://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf (accessed 17 February 2021).

[9] Global Internet Protocol (IP) traffic, a proxy for data flows, grew from about 100 gigabytes (GB) per day in 1992 to more than 45,000 GB per second in 2017 – and yet the world is only in the early days of the data-driven economy; by 2022 global IP traffic is projected to reach 150,700 GB per second, fuelled by more and more people accessing online services for the first time, and by the expansion of the Internet of Things. See UNCTAD, *Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries*, UNCTAD/DER/2019 (Overview) (2019), available at https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf (accessed 17 February 2021).

[10] J. Ferencz and J. López González, *Digital Trade and Market Openness*, OECD Trade Policy Papers, 217 (2018), available at https://www.oecd-ilibrary.org/trade/digital-trade-and-market-openness_1bd89c9a-en (accessed 28 October 2020).

[11] WTO, *supra* note 7.

[12] WTO, *Electronic Commerce*, available at https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm (accessed 18 January 2021).

[13] M. Valente, *Digital Technologies and Copyright: International Trends and Implications for Developing Countries*, Digital Pathways at Oxford Paper Series; *No. 1.* (2020), available at https://pathwayscommission.bsg.ox.ac.uk/Mariana-Valente-digital-technologies-and-copyright.

[14] OECD, WTO and IMF, *Handbook on Measuring Digital Trade* (2020) 156, available at https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf (accessed 17 February 2021).

[15] Y. Ismail, *E-Commerce in the World Trade Organization: History and Latest Developments in the Negotiations under the Joint Statement* (2020) 34, available at https://www.iisd.org/system/files/publications/e-commerce-world-trade-organization-.pdf (accessed 18 January 2021).

[16] M. Burri, 'Data Flows and Global Trade Law', *SSRN Electronic Journal* (2020), available at https://ssrn.com/abstract=3634434 (accessed 17 February 2021).

[17] For a detailed analysis of TiSA see Gao, 'Digital or Trade? The Contrasting Approaches of China and US to Digital Trade', 21 *Journal of International Economic Law* (2018) 297.

[18] Ismail, *supra* note 15; WTO, 'Negotiations on E-Commerce Continue, Eyeing a Consolidated Text by the End of the Year', *World Trade Organization News* (2020), available at https://www.wto.org/english/news_e/news20_e/ecom_26oct20_e.htm (accessed 1 November 2020).

[19] WTO, *supra* note 18.

[20] Willemyns, 'Agreement Forthcoming? A Comparison of EU, US, and Chinese RTAs in Times of Plurilateral E-Commerce Negotiations', 23 *Journal of International Economic Law* (2020) 221.

[21] Burri, *supra* note 16.

[22] Z. Smart, *Call to Action at Riyadh International Standards Summit*, 5 November 2020, World Standards Cooperation, available at https://www.worldstandardscooperation.org/2020/11/05/call-to-action-at-riyadh-international-standards-summit/#more-1502 (accessed 5 February 2021).

[23] A. Beattie, 'Technology: How the US, EU and China Compete to Set Industry Standards', *Financial Times* (2019), available at https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271 (accessed 5 February 2021].

[24] European Commission, Exchanging and Protecting Personal Data in a Globalised World, 10 January 2017.

[25] UNCTAD, *supra* note 9.

[26] M. Cartwright, 'Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle', *Internet Policy Review* (2020), available at https://policyreview.info/articles/analysis/internationalising-state-power-through-internet-google-huawei-and-geopolitical (accessed 1 November 2020).

[27] I. Manak, *U.S. WTO E-Commerce Proposal Reads Like USMCA*, 8 May 2019, International Economic Law and Policy Blog, available at https://worldtradelaw.typepad.com/ielpblog/2019/05/us-wto-e-commerce-proposal-reads-like-usmca.html (accessed 1 November 2020).

[28] D. Sevastopulo, 'Judge Blocks Trump's App Store Ban on TikTok', *Financial Times*, 28 September 2020, available at https://www.ft.com/content/84c73841-ef42-4d97-8a6e-b7d02d5fda20 (accessed 18 January 2021).

[29] UNCTAD, *Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries*, UNCTAD/DER/2019 (Overview) (2019), available at https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf (accessed 17 February 2021).

[30] A. Bradford, *The Brussels Effect: How the European Union Rules the World* (2020).

[31] EU, *Adequacy Decisions*, available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 2 November 2020). The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.

[32] United States Trade Representative, *2020 National Trade Estimate Report on Foreign Trade Barriers*, 2020.

[33] Bradford, *supra* note 30. At 140.

[34] Following EU proposals, for instance, the new EU-UK trade agreement contains a stand-alone article on the 'right to regulate' whereby "The Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity" (art. DIGIT.3 TCA).

[35] Velli, 'The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements', 2019 4 *European Papers - A Journal on Law and Integration* (2019) 881894.

[36] European Commission, Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, 2018.

[37] European Commission, Press Release: *EU and China Reach Agreement in Principle on Investment*, 30 December 2020, European Commission, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2541 (accessed 18 January 2021).

[38] Bauer and Erixon, 'Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls', *ECIPE European Centre for International Political Economy - No. 2/2020* (2020), available at https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf (accessed 1 November 2020).

[39] *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*, European Commission, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en (accessed 18 January 2021); *The Digital Markets Act: Ensuring Fair and Open Digital Markets*, European Commission, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (accessed 18 January 2021).

[40] Gao, *supra* note 17.

[41] *Ibid.*

[42] *Internet Companies Ranked by Revenue 2019*, June 2020, Statista, available at https://www.statista.com/statistics/277123/internet-companies-revenue/ (accessed 19 January 2021).

[43] Kynge and Liu, 'From AI to Facial Recognition: How China Is Setting the Rules in New Tech', *Financial Times* (2020), available at https://www.ft.com/content/188d86df-6e82-47eb-a134-2e1e45c777b6 (accessed 1 November 2020).

[44] The other two Chinese companies on the list – that is, Tencent and Baidu – provide, respectively social networking and search services. While they are often referred to respectively as the Facebook and the Google of China, they do not share the demands by the latter group for rules on cross-border digital trade because they are not global companies like their US counterparts. Instead, they serve the Chinese market almost exclusively and most of their facilities and operations are based in China. Gao, *supra* note 17.

[45] *Ibid.*

[46] P. Leblond, *Digital Trade: Is RCEP the WTO's Future?*, 23 November 2020, Centre for International Governance Innovation, available at https://www.cigionline.org/articles/digital-trade-rcep-wtos-future (accessed 18 January 2021).

[47] N. Liu, M. Ruehl and R. McMorrow, 'China Draws up First Antitrust Rules to Curb Power of Tech Companies', *Financial Times,* 10 November 2020, available at https://www.ft.com/content/1a4a5001-6411-45fa-967c-0fd71ba9300b (accessed 18 January 2021).

[48] Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement', 33 *Harvard Journal of Law & Technology* (2020) 31.

[49] D. Elms, 'Unpacking the Digital Economy Partnership Agreement (DEPA)', 28 January 2020, *Talking Trade*, available at http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa (accessed 17 February 2021).

[50] Singapore government, 'Joint Ministerial Statement: Singapore Leads the Way in the New Digital Economy Partnership Agreement with Chile and New Zealand', (2019), available at https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Digital-Economy-Partnership-Agreement/Press-release-on-the-start-of-DEPA-negotiations--May-2019.pdf (accessed 1 November 2020).

[51] DEPA Signing Text, 11 June 2020.

[52] Burri, *supra* note 16.

[53] UNCTAD, *supra* note 29.

[54] UNCTAD, *Competition Issues in the Digital Economy*, Intergovernmental Group of Experts on Competition Law and Policy, 18th session (2019), available at https://unctad.org/meetings/en/SessionalDocuments/ciclpd54_en.pdf (accessed 17 February 2021).

[55] Mattoo and Meltzer, 'International Data Flows and Privacy: The Conflict and Its Resolution', 21 *Journal of International Economic Law* (2019) 769.

[56] UNCTAD, *supra* note 9.

[57] Meltzer, 'The United States-Mexico-Canada Agreement: Developing Trade Policy for Digital Trade', XI *Trade Law & Development* (2019) 239.

[58] UNCTAD, *supra* note 9.

[59] Burri, *supra* note 16.

[60] Yakovleva and Irion, 'Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade', 10 *International Data Privacy Law* (2020) 201. At 211.

[61] *Ibid.*

[62] Burri, *supra* note 16.

[63] Bauer and Erixon, *supra* note 38.

[64] Yakovleva and Irion, *supra* note 60.

[65] *Ibid.* The precise wording is "information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection" (art. 19.2.3).

[66] See an excellent discussion of Article XIV in Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?', 19 *World Trade Review* (2020) 341.

[67] J. McGregor, 'NAFTA Talks: U.S. Proposal for Cross-Border Data Storage at Odds with B.C., N.S. Law', *CBC* (2017), available at https://www.cbc.ca/news/politics/nafta-data-storage-privacy-1.4220272 (accessed 1 November 2020).

[68] In the Financial Services Chapter the Parties commit that "No Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory". It further notes that "Each Party shall, to the extent practicable, provide a covered person with a reasonable opportunity to remediate a lack of access to information … before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of another jurisdiction' (art. 17.18 USMCA). A similar provision is found in the US–Japan agreement, although it also introduces a requirement that a Party must consult with the other Party before localisation measures are introduced (art. 8.63 US–Japan).

[69] Sidley Austin LLP, *Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and the United States*, 2016. Available at https://www.sidley.com/en/insights/publications/2016/01/essentially-equivalent (accessed 10 October 2020). The foundations of the right to privacy in the US can be found in the Fourth Amendment to the Bill of Rights of 1791, which protected people against unreasonable government searches and seizures. The right to privacy as a legal concept was later established in the seminal work by Warren and Brandeis, published in 1890, which alluded to a "right to be left alone". For example, the Privacy Act of 1974 seeks to regulate comprehensively personal data processing, but its application is restricted to the activities of federal government departments and agencies, and does not apply to private actors. The Gramm-Leach-Bliley Act protects personal financial records kept by financial institutions, and the Children's Online Privacy Protection Act (COPPA) governs the collection of personal data from children online.

[70] Yakovleva and Irion, *supra* note 60. The Federal Trade Commission (FTC) enforces targeted (or vertical) statutes that protect information relating to health, credit, and other financial matters, as well as online information on children. The FTC has enforcement powers over privacy-related contractual provisions, such as the power to issue orders and seek consumer redress in certain circumstances, but federal law does not stipulate what those provisions should be.

[71] Mattoo and Meltzer, *supra* note 55, at 785.

[72] In a footnote it states that a Party may comply with the obligation in this paragraph by "adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy".

[73] On APEC approach see 22-23 of Mattoo and Meltzer, *supra* note 55.

[74] Charter of Fundamental Rights of the European Union (articles 7 and 8); TEUF (article 16); Europe Convention 108 (article 1); European Convention on Human Rights (article 8).

[75] Regulation (EU) 2016/679.

[76] Schrems v. Data Protection Commissioner 2015 and 2020. On Schrems II see Chander, 'Is Data Localization a Solution for Schrems II?', *SSRN Electronic Journal* (2020), available at http://dx.doi.org/10.2139/ssrn.3662626 (accessed 17 February 2021); European Commission, *supra* note 24.

[77] European Commission, *Adequacy Decisions*, European Commission, available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 18 January 2021).

[78] Mattoo and Meltzer, *supra* note 55.

[79] Yakovleva and Irion, *supra* note 60.

[80] The CJEU has already invalidated two adequacy decisions issued by the European Commission for data transfers to the US. In 2015, the Court invalidate the EU–US Safe Harbour, in a ruling known as Schrems I (Maximillian Schrems v. Data Protection Commissioner – Case C-362/14). In 2020, a second ruling invalidated the invalidated the adequacy decision underlying the EU–US Privacy Shield arrangement, known as Schrems II (Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems – Case C-311/18).

[81] J. P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security*, 5 August 2020, VoxEU, available at https://voxeu.org/article/impact-gdpr-data-flows-and-national-security (accessed 17 February 2021).

[82] Standard Contractual Clauses contractually bind third parties that receive the personal data of EU citizens to provide privacy protections consistent with GDPR. Binding Corporate Rules do the same, but for entities in a conglomerate receiving such data.

[83] Case C-311/18, para. 134 "It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."

[84] Meltzer, *supra* note 81.

[85] Yakovleva and Irion, *supra* note 60.

[86] European Commission, *Draft Text of the Agreement on the New Partnership with the United Kingdom*, UKTF (2020), available at https://ec.europa.eu/info/sites/info/files/200318-draft-agreement-gen.pdf (accessed 2 November 2020).

[87] Yakovleva and Irion, *supra* note 60.

[88] EU, Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, 26 April 2019.

[89] Aaronson and Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO', 21 *Journal of International Economic Law* (2018) 245.

[90] *Ibid.*

[91] X. Liu, *China's Hyperactive Debates on Personal Data Protection*, 18 December 2020, available at https://thediplomat.com/2020/12/chinas-hyperactive-debates-on-personal-data-protection/ (accessed 18 January 2021); D. Zhang and N. Zhang, *China Draft Personal Information Protection Law ('PIPL')*, 3 November 2020, Fieldfisher, available at https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/china-draft-personal-information-protection-law-pipl (accessed 18 January 2021).

[92] "The UK will in future develop separate and independent policies in areas such as (but not limited to) the points-based immigration system, competition and subsidy policy, the environment, social policy, procurement, and data protection, maintaining high standards as we do so", Prime Minister, Statement UIN HCWS86, 3 February 2020. Available at https://questions-statements.parliament.uk/written-statements/detail/2020-02-03/HCWS86 (accessed 7 October 2020).

[93] Ministry of Foreign Affairs of Japan, *Japan-UK Comprehensive Economic Partnership Agreement*, available at https://www.mofa.go.jp/ecm/ie/page24e_000270.html (accessed 26 October 2020).

[94] For example, the UK–Japan agreement article on privacy stipulates that each Party "shall" publish information on the personal information protections it provides to users of electronic commerce whereas the CPTPP text read "should".

[95] Department for International Trade, UK, *Final Impact Assessment of the Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan for a Comprehensive Economic Partnership*, (2020), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929059/final-impact-assessment-UK-Japan-comprehensive-economic-partnership.pdf (accessed 17 February 2021).

[96] The UK has conferred adequacy on the EU on a transitional basis under the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019 No. 419) – see paragraphs 4 and 5 of Schedule 21 to the Data Protection Act 2018 as inserted by paragraph 102 of Schedule 2 to SI 2019 No. 419. This enables a free flow of data to continue from the UK to the EU after the end of the transition period. UK Parliament, The Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations 2019, UK Statutory Instruments. Also see: Minister John Whittingdale, HC Deb, 29 September 2020, cW. Available at https://questions-statements.parliament.uk/written-questions/detail/2020-09-24/95167 (accessed 7 October 2020).

[97] E. Duhs, *EU-UK Data Flows, Adequacy and Regulatory Changes from 1 January 2021*, 24 December 2020, Fieldfisher, available at https://www.fieldfisher.com/en/insights/an-adequate-agreement-what-the-brexit-deal-means-f (accessed 5 February 2021).

[98] New Economics Foundation and UCL European Institute, *The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure and EU Adequacy Decision* (2020), available at https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf (accessed 5 February 2021).

[99] Para 20 House of Commons, *The Need for Progress in the Negotiations* (2020), available at https://committees.parliament.uk/publications/1538/documents/14358/default/ (accessed 17 February 2021).

[100] Murray, 'Data Transfers between the EU and UK Post Brexit?', 7 *International Data Privacy Law* (2017) 149.

[101] The CJEU has already invalidated two adequacy decisions issued by the European Commission for data transfers to the US. In 2015, the Court invalidate the EU–US Safe Harbour, in a ruling known as Schrems I (Maximillian Schrems v. Data Protection Commissioner – Case C-362/14). In 2020, a second ruling invalidated the invalidated the adequacy decision underlying the EU–US Privacy Shield arrangement, known as Schrems II (Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems – Case C-311/18).

[102] This willingness of the CJEU to offer discretion to European authorities to balance rights to privacy and security was informed by jurisprudence from the European Court of Human Rights (ECHR), but when it came to the US in Schrems II, the CJEU rejected ECHR jurisprudence as relevant, leading the court to apply a relatively more rigid application of its "proportionality" principle, requiring that limitations on EU privacy rights be "strictly necessary". J. P. Meltzer, *Why Schrems II Requires US-EU Agreement on Surveillance and Privacy*, 8 December 2020, Brookings, available at https://www.brookings.edu/techstream/why-schrems-ii-requires-us-eu-agreement-on-surveillance-and-privacy/ (access 18 January 2021).

[103] Murray, *supra* note 100.

[104] Interestingly, the EU as a whole has no competence with regard to national security. Under EU law, national security is the sole responsibility of member states, who also have discretion to establish "necessary and proportionate" limits to the right to privacy. As argued by Meltzer (2020), "in effect, each EU state is given the discretion to balance national security needs with data privacy rights. Yet, the EU is not according a similar discretion to third countries". In fact, due to the lack of uniform approach, some argue that US law, following the Snowden revelations, offer better controls over government surveillance than the ones available under EU law. G. Robertson, *Opinion of Geoffrey Robertson QC for Facebook*, 14 January 2016, available at https://www.bcl.com/downloads/RobertsonSafeHarbour.pdf (accessed 17 February 2017).

[105] *Commission Implementing Decision (EU) 2019/ of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan under the Act on the Protection of Personal Information*, 19 March 2019 58, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419&from=EN (accessed 17 February 2021).

[106] Yakovleva and Irion, *supra* note 60.

[107] European Data Protection Board, 'Letter Regarding the Agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime', (2020), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf (accessed 17 February 2021).

[108] G. Greenleaf, *Japan: EU Adequacy Discounted*, SSRN Scholarly Paper, ID 3276016 (2018), available at https://papers.ssrn.com/abstract=3276016 (accessed 17 February 2021); Also see Wang, *supra* note 48.

[109] For an argument that these obligations are not consistent, see G. Greenleaf, *Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108*, SSRN Scholarly Paper, ID 3352288 (2018), available at https://papers.ssrn.com/abstract=3352288 (accessed 5 February 2021).

[110] Duhs, *supra* note 97.

[111] *Ibid.*

[112] Wu, 'Network Neutrality, Broadband Discrimination', 2 *Journal on Telecommunications & High Technology Law* (2003) 141.

[113] Measures to manage internet traffic are usually allowed in very limited exceptional cases, such as for legal, security or emergency reasons.

[114] See Aaronson and Leblond, *supra* note 89.

[115] *The Open Internet Access (Amendment Etc) (EU Exit) Regulations 2018*, GOV.UK, available at https://www.gov.uk/eu-withdrawal-act-2018-statutory-instruments/the-open-internet-access-amendment-eu-exit-regulations-2018 (accessed 28 October 2020).

[116] See Romero Moreno, ''Upload Filters' and Human Rights: Implementing Article 17 of the Directive on Copyright in the Digital Single Market', 34 *International Review of Law, Computers & Technology* (2020) 153; Seng, 'The State of the

Discordant Union: An Empirical Analysis of DMCA Takedown Notices', *SSRN Electronic Journal* (2014), available at http://www.ssrn.com/abstract=2411915 (accessed 7 November 2020).

[117] The FT View, 'New Realities Confront a Maturing Internet', *Financial Times* (2017), available at https://www.ft.com/content/33e0372c-96f9-11e7-b83c-9588e51488a0 (accessed1 November 2020).

[118] F. Gillette, 'Section 230 Was Supposed to Make the Internet a Better Place. It Failed', *Bloomberg Businessweek* (2019), available at https://www.bloomberg.com/news/features/2019-08-07/section-230-was-supposed-to-make-the-internet-a-better-place-it-failed (accessed 17 February 2021); Wakabayashi, 'Legal Shield for Websites Rattles Under Onslaught of Hate Speech', *New York Times* (2019), available at https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html (accessed 17 February 2021).

[119] CEO's from Facebook, Twitter and Google gave testimony to the US Senate on 28 October 2020. Mark Zuckerberg, for example, argued that with the removal of the section, technology companies would be more likely to censor content in order to avoid being held responsible for hate speech and harassment. Twitter's Jack Dorsey said that changing the rule will make it more difficult for small platforms to survive, due to the high compliances costs associated with monitoring content, and that internet communication will be, as a result, controlled by a small number of large companies. Lima, 'Facebook Embraces Updating Tech's Legal Shield While Twitter, Google Urge Restraint', *Politico* (2020), available at https://www.politico.com/news/2020/10/27/facebook-twitter-google-hearing-legal-shield-432903 (accessed 18 February 2021).

[120] EFF, *Section 230 of the Communications Decency Act*, Electronic Frontier Foundation, available at https://www.eff.org/issues/cda230 (accessed 17 February 2021); Letter from Scholars Regarding NAFTA and S.230, 21 January 2018.

[121] M. Kelly, 'Joe Biden Wants to Revoke Section 230', *The Verge* (2020), available at https://www.theverge.com/2020/1/17/21070403/joe-biden-president-election-section-230-communications-decency-act-revoke (accessed 1 November 2020).

[122] Ending Support for Internet Censorship Act, S. 194, 116th Cong., 2019

[123]See: US Congress, S.1914 - Ending Support for Internet Censorship Act, 2020-2019; US DoJ, Proposed Section 230 Legislation, 23 September 2020; US Government, Executive Order on Preventing Online Censorship, 28 May 2020.

[124] K. Browning, 'Zuckerberg and Dorsey Face Harsh Questioning From Lawmakers', *The New York Times*, 6 January 2021, available at https://www.nytimes.com/live/2020/11/17/technology/twitter-facebook-hearings (accessed 17 February 2021).

[125] O'Connell and Bakina, 'Using IP Rights to Protect Human Rights: Copyright for 'Revenge Porn' Removal', 40 *Legal Studies* (2020) 442.

[126] A. Menjivar and Access Now, Warning: Repressive regimes are using DMCA takedown demands to censor activists, (blog), 22 October 2020, available at https://www.accessnow.org/dmca-takedown-demands-censor-activists/ (accessed 17 February 2021).

[127] U.S. Copyright Office, *Section 512 Study*, 21 May 2020, available at https://www.copyright.gov/policy/section512 (accessed 17 February 2021).

[128] The USMCA requires that "no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information" (art.19.17.2 USMCA). It also establishes that service providers will not be held liable "on account of any action voluntarily taken in good faith" to restrict access to or availability of material that the supplier or user considers to be harmful or objectionable; or "for any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable." (art.19.17.3 USMCA).

[129] In 2019, the Senate introduced a bill to prohibit large social media companies from moderating "politically biased" information on their platform (Ending Support for Internet Censorship Act, S. 194, 116th Cong., 2019). The critique of s.230 also underlies the executive order issued by President Trump on "Preventing Online Censorship" from May 2020. In September 2020, the Department of Justice sent draft legislation to Congress to execute the presidential directive and to reform the DCA. See: US Congress, S.1914 - Ending Support for Internet Censorship Act, 2020-2019; US DoJ, Proposed Section 230 Legislation, 23 September 2020; US Government, Executive Order on Preventing Online Censorship, 28 May 2020.

[130] K. Madigan, 'NAFTA Shouldn't Include Outdated Internet Safe Harbors', *The Hill* (2018), available at https://thehill.com/opinion/technology/370956-nafta-shouldnt-include-outdated-internet-safe-harbors (accessed 17 February 2021); N. Turkewitz, *NAFTA: Preserving the Status Quo & Inviting a Future That We Are Incapable of Shaping*, 31 August 2018, Medium, available at https://medium.com/@nturkewitz_56674/nafta-preserving-the-status-quo-inviting-a-future-that-we-are-incapable-of-shaping-ff4c2ad0890e (accessed 1 November 2020).

[131] 'Letter from Congressional House Judiciary Committee', (2019), available at https://judiciary.house.gov/sites/democrats.judiciary.house.gov/files/documents/ambassador%20lighthizer%20usmca%20letter%209.17.19.pdf?utm_campaign=84-519 (accessed 17 February 2021).

[132] Article 14 of the e-Commerce Directive establishes that three types of intermediaries are excluded from liability, provided they meet the qualifying conditions: mere conduit, caching; and hosting. The services provided by internet platforms such as Google are usually framed under the hosting provision.

[133] European Commission, *The Digital Services Act Package*, 15 December 2020, available at https://ec.europa.eu/digital-single-market/en/digital-services-act-package (accessed 17 February 2021).

[134] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, 15 December 2020.

[135] Electronic Frontier Foundation, *European Commission's Proposed Digital Services Act Got Several Things Right, But Improvements Are Necessary to Put Users in Control*, 15 December 2020, available at https://www.eff.org/deeplinks/2020/12/european-commissions-proposed-regulations-require-platforms-let-users-appeal (accessed 17 January 2021).

[136] Article 2(6) of the Copyright Directive defines online content-sharing service provider as: "a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes. Providers of services, such as not-for-profit online encyclopaedias, not-for-profit educational and scientific repositories, open-source software developing and sharing platforms, providers of electronic communications services as defined in Directive (EU) 2018/1972, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not 'online content-sharing service providers' within the meaning of this Directive".

[137] Curto, 'EU Directive on Copyright in the Digital Single Market and ISP Liability: What's Next at International Level?', 11 *Journal of Law, Technology and the Internet,* (2020) 84.

[138] In response to this criticism, the final version of the Directive introduced considerations related to the size of the provider, the amount of content uploaded, but critics argue they might not be sufficient to address the matter. Valente, *supra* note 13.

[139] EU, *supra* note 88.

[140] Freedom House, *China's New Leaders Refine Internet Control* (2013), available at https://freedomhouse.org/report/special-report/2013/chinas-new-leaders-refine-internet-control (accessed 18 January 2021).

[141] L. Ruan, *Regulation of the Internet in China: An Explainer*, 7 October 2019, Asia Dialogue, available at https://theasiadialogue.com/2019/10/07/regulation-of-the-internet-in-china-an-explainer/ (accessed 18 January 2021); M. Shi, *What China's 2018 Internet Governance Tells Us About What's Next*, 28 January 2019, New America, available at http://newamerica.org/cybersecurity-initiative/digichina/blog/what-chinas-2018-internet-governance-tells-us-about-whats-next/ (accessed 18 January 2021).

[142] State Council Information Office, *The State of the Internet in China*, 8 June 2010, available at http://www.gov.cn/zhengce/2010-06/08/content_2615774.htm (accessed 18 January 2021).

[143] For example, the Provisions on the Administration of Microblog Information Services (http://en.pkulaw.cn/display.aspx?cgid=309714&lib=law); Provisions for the Administration of Internet News Information Services (http://en.pkulaw.cn/display.aspx?cgid=8d18a3f4334a2686bdfb&lib=law); and Regulations for the Security Assessment of Internet Information Services Having Public Opinion Properties or Social Mobilization Capacity (https://www.newamerica.org/cybersecurity-initiative/digichina/blog/new-rules-target-public-opinion-and-mobilization-online-china-translation/).

[144] Cybersecurity Law of the People's Republic of China.

[145] Friedmann and Frosio, 'China's IP Regulation and Omniscient Intermediaries: Oscillating from Safe Harbour to Liability', in *Oxford Handbook of Online Intermediary Liability* (2020).

[146] *Ibid.*

[147] Department for Digital, Culture, Media & Sport, UK, *Online Harms White Paper* (2019), available at https://www.gov.uk/government/consultations/online-harms-white-paper (accessed 17 February 2021); J. Woodhouse, M. Lalic and S. Lipscombe, *Research Briefing: Online Harms*, 1 October 2020, House of Commons Library, available at https://commonslibrary.parliament.uk/research-briefings/cdp-2020-0093/ (accessed 17 February 2021).

[148] Department for Digital, Culture, Media & Sport, and Home Office, UK, *Online Harms White Paper: Full Government Response to the Consultation* (2020), available at https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response (accessed 17 February 2021).

[149] *Ibid.*

[150] As pointed out by Nash, given the wide breadth of issues described in the OHWP, conflating illegal and legal-but-harmful content, the "idea that a single effective and proportionate regulatory approach could be designed in such a way as to tackle every one of these matters is highly presumptuous and neglects the wide array of complex social factors underpinning the production, sharing and engagement of such content"; Nash, 'Revise and Resubmit? Reviewing the 2019 Online Harms White Paper', 11 *Journal of Media Law* (2019) 18.

[151] I. Barber, *The UK Government's Full Response to the Online Harms White Paper: Initial Thoughts*, 16 December 2020, Global Partners Digital, available at https://www.gp-digital.org/the-uk-governments-full-response-to-the-online-harms-white-paper-initial-thoughts/ (accessed 17 February 2021); ORG, *ORG Policy Responses to Online Harms White Paper* (2019), Open Rights Group, available at https://www.openrightsgroup.org/publications/org-policy-responses-to-online-harms-white-paper/ (accessed 17 February 2021).

[152] Woodhouse, Lalic and Lipscombe, *supra* note 147.

[153] UK Government, UK-EU Trade and Cooperation Agreement: Summary, December 2020.

[154] Procedural obligations are concerned with proceedings to be adopted by the Parties. They include, for example, obligations to promote dialogue, to give information to specific actors, to respect a deadline, to enter into negotiations, to behave 'in good faith', among others. See Okowa, 'Procedural Obligations of States', in *State Responsibility for Transboundary Air Pollution in International Law* (2000).

[155] UK Department for International Trade, *UK-US Free Trade Agreement*, 2020, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869592/UK_US_FTA_negotiations.pdf (accessed 4 September 2020).

[156] USTR, United States-United Kingdom Negotiations: Summary of Specific Negotiating Objectives, February 2019.

[157] T. Cross, 'Trade Talks with the US Could Scupper the UK's Online Harms Bill', 9 September 2020, *VideoWeek*, available at https://videoadnews.com/2020/09/09/trade-talks-with-the-us-could-scupper-the-uks-online-harms-bill/ (accessed 26 October 2020).

[158] ''Procedural accountability' would require governments to have the ability to hold platforms accountable for the processes, private policies and systems they put in place. See Bunting, 'From Editorial Obligation to Procedural Accountability: Policy Approaches to Online Content in the Era of Information Intermediaries', 3 *Journal of Cyber Policy* (2018) 165; Nash and Bunting, 'A Policy Playbook for Platforms', 46 *InterMEDIA* (2018), available at https://www.iicom.org/wp-content/uploads/im-july2018-policyplaybook-min.pdf (accessed 17 February 2021).

[159] Krishnamurthy and Fjeld, 'CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States', *SSRN Electronic Journal* (2020), available at https://www.ssrn.com/abstract=3645462 (accessed October 2020); *Ibid.*

[160] Krishnamurthy and Fjeld, *supra* note 159. *Ibid.*

[161] Liberal Party of Canada, *Online Hate Speech, Exploitation and Harassment Online*, available at https://liberal.ca/our-platform/online-hate-speech-exploitation-and-harassment-online/ (accessed 17 February 2021).

[162] Krishnamurthy and Fjeld, *supra* note 159.

[163] J. Camarena, *Mexico*, Wilmap, The Center for Internet and Society, Stanford Law School, available at https://wilmap.law.stanford.edu/country/mexico (accessed 17 February 2021).

[164] Centre for Data Ethics and Innovation, *Review into Bias in Algorithmic Decision-Making* (2020), available at https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making (accessed 17 February 2021).

[165] W. Bedingfield, 'Everything That Went Wrong with the Botched A-Levels Algorithm', *WIRED* (2020), available at https://www.wired.co.uk/article/alevel-exam-algorithm (accessed 17 February 2021).

[166] Wachter, Mittelstadt and Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR', 31 *Harvard Journal of Law and Technology* (2018) 841.

[167] ITUC, *E-Commerce Free Trade Agreements, Digital Chapters and the Impact on Labour* (2019), available at https://www.ituc-csi.org/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf (accessed 17 February 2021).

[168] The Alan Turing Institute, *A Right to Explanation*, available at https://www.turing.ac.uk/research/impact-stories/a-right-to-explanation (accessed 17 February 2021).

[169] Mittelstadt, Russell and Wachter, 'Explaining Explanations in AI', in *Proceedings of the Conference on Fairness, Accountability, and Transparency* (2019) 279; Science and Technology Committee, House of Commons, *Algorithms in Decision-Making*, Fourth Report of Session 2017-2019 (2018) 52, at 28; Wachter, Mittelstadt and Russell, *supra* note 166.

[170] WTO and EU, *Joint Statement on Electronic Commerce: Establishing an Enabling Environment for Electronic Commerce* (2018), available at https://trade.ec.europa.eu/doclib/docs/2018/october/tradoc_157457.pdf (accessed 17 February 2021); J. Ruiz, *US Red Lines for Digital Trade with the UK Cause Alarm*, 14 March 2019, Open Rights Group, available at https://www.openrightsgroup.org/blog/us-red-lines-for-digital-trade-with-the-uk-cause-alarm/ (accessed 29 October 2020).

[171] EU, *White Paper on Artificial Intelligence: A European approach to excellence and trust*, (2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 17 February 2021).

[172] Wachter, Mittelstadt and Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', 7 *International Data Privacy Law* (2017) 76.

[173] European Commission, *supra* note 134.

[174] UK Government, *supra* note 148.

[175] S I. Sample, 'AI Watchdog Needed to Regulate Automated Decision-Making, Say Experts', The Guardian, 28 January, 2017, available at https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions (accessed 17 February 2021).

[176] H. Lee-Makiyama, *Briefing Note: AI & Trade Policy*, Tallinn Digital Summit (2018), available at https://ecipe.org/wp-content/uploads/2018/10/TDS2018-BriefingNote_AI_Trade_Policy.pdf (accessed 17 February 2021).

[177] During the negotiation of the TPP, there were concerns that the provision banning governments from requiring access to source code would restrict US regulators' access to information necessary to audit firms, limiting their ability to evaluate deceitful practices as well as security flaws in several industries, including auto manufacturers. K. Finley, 'Trade Pact Could Bar Governments From Auditing Source Code', *Wired* (2015), available at https://www.wired.com/2015/11/trade-pact-could-bar-governments-from-auditing-source-code/ (accessed 3 February 2021).

[178] Wachter, Mittelstadt and Russell, *supra* note 166.

[179] Guglya and Maciel, *Addressing the Digital Divide in the Joint Statement Initiative on E-Commerce: From Enabling Issues to Data and Source Code Provisions*, International Institute for Sustainable Development and CUTS International, (2020) 97.

[180] T. Moran, *Should US Tech Companies Share Their "Source Code" with China?*, 28 October 2015, PIIE, available at https://www.piie.com/blogs/china-economic-watch/should-us-tech-companies-share-their-source-code-china (accessed 3 February 2021).

[181] WTO, *supra* note 7.

[182] *Ibid.*

[183] Valente, *supra* note 13.

[184] WTO, *supra* note 7.

[185] J. Tirole, *Economics for the Common Good* (2017).

[186] WTO, *supra* note 7.

[187] UK Government, Security Considerations When Coding in the Open, 2017.

[188] R. S. Neeraj, *Trade Rules on Source Code: Deepening the Digital Inequities by Locking up the Software Fortress*, WTO, (2017), available at http://rgdoi.net/10.13140/RG.2.2.25509.19681 (accessed 2 February 2021).

[189] Ruiz, *supra* note 170.

[190] EU, *Open Source Software Strategy*, (2020), available at https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en (accessed 3 February 2021).

[191] US Government, *Open Source Code*, U.S. Department of Commerce, available at https://www.commerce.gov/about/policies/source-code (accessed 3 February 2021).

[192] S, *supra* note 188.

[193] Meltzer, 'Governing Digital Trade', 18 *World Trade Review* (2019) S23.

[194] EU, *supra* note 169.

[195] Huang and Smith, 'China's Record on Intellectual Property Rights Is Getting Better and Better', *Foreign Policy* (2019), available at https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/ (accessed 17 February 2021).

[196] Intellectual Property Office, British Embassy Beijing and Department for International Trade, UK, *Intellectual Property and Industrial Software in China* (2019), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784777/FINAL_-_IP_and_Industrial_Software_in_China_factsheet_-_March_2019.pdf (accessed 17 February 2021).

[197] Lee, 'Hacking Into China's Cybersecurity Law', 53 *Wake Forest Law Review* (2017) 48.

[198] Ido, 'Intellectual Property and Electronic Commerce: Proposals in the WTO and Policy Implications for Developing Countries', Policy Brief No. 62 *South Centre* (2019) 8.

[199] Valente, *supra* note 13.

[200] Ruiz, 'Open Rights Group Submission to UK Consultation on a New Free Trade Agreement with the United States of America', (2018) 9.

[201] USTR, *supra* note 156.

[202] WTO, E-Commerce, Trade and the Covid-19 Pandemic, 4 May 2020.

[203] UNCTAD, 'UNCTAD Estimates of Global E-Commerce 2018', *UNCTAD Technical Notes on ICT for Development* (2020), available at https://unctad.org/system/files/official-document/tn_unctad_ict4d15_en.pdf (accessed 17 February 2021).

[204] *Ibid.*

[205] WEF, 'Making Deals in Cyberspace: What's the Problem?', *World Economic Forum* (2017), available at http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf (accessed 1 November 2020).

[206] The EU established a new legal structure for electronic identification, signatures, seals and documents in July 2016, known as the Regulation on electronic identification and trust services (eIDAS Regulation). The Regulation provides for three levels of signatures: basic, advanced and qualified e-signatures. While all types of signature are legal, admissible and enforceable, only qualified e-signatures are legally identical to handwritten signatures. These are also the only types of signatures mutually recognised by all EU member states. Qualified electronic certificates must be based on qualified certificates issued by a CA accredited and supervised as designed by EU member states. *Ibid.*

[207] The EU established a new legal structure for electronic identification, signatures, seals and documents in July 2016, known as the regulation on electronic identification and trust services (eIDAS Regulation). The Regulation provides for three levels of signatures: basic, advanced and qualified e-signatures. While all types of signature are legal, admissible and enforceable, only qualified e-signatures are legally identical to handwritten signatures. These are also the only types of signatures mutually recognised by all EU member states. Qualified electronic certificates must be based on qualified certificates issued by a certificate authority accredited and supervised as designed by EU member states. *Ibid.*

[208] *Ibid.*

[209] Key definitions. **Electronic signatures:** The technologies used for e-signatures include email addresses, enterprise IDs, personal ID numbers (PINs), biometric identification, social IDs, scanned copies of handwritten signatures and clickable "I accept" boxes. **Digital signature:** A digital signature, or advanced e-signature, uses cryptography to scramble signed information into an unreadable format and decodes it again for the recipient. **Digital authentication** refers variously to the techniques used to identify individuals, confirm a person's authority or prerogative, or offer assurance on the integrity of information. Digital authentication can rely on a varied set of factors, such as those concerning knowledge (eg passwords, answers to a pre-selected security question), ownership (eg possession of a one-time password) or inherence (eg biometric information). Depending on the level of security desired, a digital authentication system could be single-, double- or multi-factor. **Digital identity** refers to a broader conception of the information used by a computer system to identify an agent, which is most frequently considered to be an individual but is also referred to as an entity, such as a corporation or a machine. Printed documents such as passports, national ID cards and driver's licences offer proof of a person's identity. Digital identities enable remote interactions between individuals by providing key information about who they are. See *Ibid.*

[210] WTO, *supra* note 18.

[211] WEF, *The Global Governance of Online Consumer Protection and E-Commerce: Building Trust,* World Economic Forum (2019), available at http://www3.weforum.org/docs/WEF_consumer_protection.pdf (accessed 1 November 2020).

[212] *Ibid.*

[213] Note that there are some minor differences between the USMCA, US–Japan, and US proposals at the WTO.

[214] EU, *supra* note 88.

[215] *Inter alia* that Parties will enact measures that proscribe fraudulent and deceptive commercial practices; require suppliers of goods and services to act in good faith and abide by fair commercial practices, including through the prohibition of charging consumers for unsolicited goods and services; require suppliers of goods or services to provide consumers with clear and thorough information regarding their identity and contact details, as well as regarding the goods or services, the transaction and the applicable consumer rights; grant consumers access to redress to claim their rights, including a right to remedies in cases where goods or services are paid and not delivered or provided as agreed. EU and Australia, EU–Australia Free Trade Agreement, 10 October 2018.

[216] J. Kelsey, *Important Differences between the Final RCEP Electronic Commerce Chapter and the TPPA and Lessons for E-Commerce in the WTO*, 10 February 2020, available at https://www.bilaterals.org/?important-differences-between-the (accessed 18 January 2021).

[217] EU, *supra* note 88. *Ibid.*

[218] techUK, *A Vision for UK Digital Trade Policy* (2020), available at https://www.techuk.org/shaping-policy/internation-trade.html (accessed 17 February 2021). *Ibid.*

[219] Declaration on Global Electronic Commerce, WT/MIN(98)/DEC/2, adopted 20 May 1998.

[220] WTO, Work Programme on Electronic Commerce, General Council Decision of 10 December 2019, WTO Doc. WT/L/1079 (2019).

[221] See discussion on 8-10 of OECD, Electronic Transmissions and International Trade – Shedding New Light on the Moratorium Debate, 4 November 2019.

[222] *Ibid.* See discussion on 8-10.

[223] Communication from India and South Africa -–The E-Commerce Moratorium: Scope and Impact, 10 March 2020; IISD, SDG Knowledge Hub, *WTO Members Highlight Benefits and Drawbacks of E-Commerce Moratorium*, 23 July 2020, SDG Knowledge Hub, available at https://sdg.iisd.org/news/wto-members-highlight-benefits-and-drawbacks-of-e-commerce-moratorium/ (accessed 17 February 2021).

[224] Valente, *supra* note 13.

[225] USTR, Initiation of Section 301 Investigations of Digital Services Taxes, 2 June 2020.

[226] A. Haines, 'This Week in Tax: EU Plans to Announce Its DST in 2021', *International Tax Review*, 18 September 2020, available at https://www.internationaltaxreview.com/article/b1nfjnlpv95dfq/this-week-in-tax-eu-plans-to-announce-its-dst-in-2021 (accessed 28 October 2020).

[227] G. C. Hufbauer and Z. Lu, *Policy Brief 19-14 Global E-Commerce Talks Stumble on Data Issues, Privacy, and More* (2019) 10.

[228] USTR, *supra* note 225.

[229] A. Williams, *US to Delay Tariff on French Goods over Digital Sales Tax*, *Financial Times*, 7 January 2021, available at https://www.ft.com/content/8b0c0f90-6222-4e40-bcad-c33a1065f3e7 (accessed 17 January 2021).

[230] G. C. Hufbauer and Z. (Lucy) Lu, *The European Union's Proposed Digital Services Tax: A De Facto Tariff*, Policy Brief 18-15 Peterson Institute for International Economics, (2018) 11, available at https://www.piie.com/system/files/documents/pb18-15.pdf (accessed 17 January 2021).

[231] Kelsey et al., *How 'Digital Trade' Rules Would Impede Taxation of the Digitalised Economy in the Global South,* Third World Network (2020), available at https://www.globaltaxjustice.org/sites/default/files/Digital%20Tax%20-TWN.pdf (accessed 1 November 2020).

[232] Noonan and Plekhanova, 'Taxation of Digital Services Under Trade Agreements', 23 *Journal of International Economic Law* (2020) 1015.

[233] S. Lowry, *Digital Services Taxes (DSTs): Policy and Economic Analysis*, Congressional Research Service, R45532 (2019), available at https://fas.org/sgp/crs/misc/R45532.pdf (last visited 17 January 2021].

[234] It is indeed 'very uncommon' for customs duties to be applied to services. See WTO Council for Trade in Services, The Work Programme on Electronic Commerce - Note by the Secretariat, 16 November 1998.

[235] Noonan and Plekhanova, *supra* note 232.

[236] Simply put, national treatment relates to discriminatory treatment towards another ember state's suppliers in comparison to the treatment afforded to national suppliers, whereas MFN relates to discriminatory treatment in comparison to the one afforded to suppliers from a third State.

[237] N. Sen, *Trade Law Analysis of EU's Digital Tax Proposal*, 2018, Linklaters, available at https://www.linklaters.com/en/insights/blogs/tradelinks/trade-law-analysis-of-eus-digital-tax-proposal (accessed 17 February 2021). See WTO Council for Trade in Services, *supra* note 234.

[238] See discussion in Noonan and Plekhanova, *supra* note 201, 1035-6.

[239] *Ibid,* 1030.

[240] *Ibid.*

[241] *Ibid.*

[242] *Ibid,* 1037.

[243] USTR, *Section 301 – Digital Services Taxes*, 14 January 2021, available at https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-digital-services-taxes (accessed 18 January 2021).

[244] D. Lawder, 'USTR Says Austria, Spain, UK Digital Taxes Discriminate against U.S. Firms', *Reuters* (2021), available at https://www.reuters.com/article/us-usa-trade-digital-tax-idUSKBN29J2AZ (accessed 18 January 2021).

[245] EU, *supra* note 88.

[246] EU and Australia, *supra* note 215.

[247] OECD/G20 Inclusive Framework on BEPS, Cover Statement by the Inclusive Framework on the Reports on the Blueprints of Pillar One and Pillar Two, 14 October 2020.

[248] See discussion on p. 47 of Kelsey et al., *supra* note 231.

[249] WTO General Council, Communication from Australia; Canada; Chile; Colombia; Hong Kong, China; Iceland; Republic of Korea; New Zealand; Norway; Singapore; Switzerland; Thailand and Uruguay, 29 June 2020, WT/GC/W/799/Rev.1.

[250] Goh and Leng, 'China Regulator Says Should Consider Digital Data Tax for Tech Firms', *Reuters* (2020), available at https://www.reuters.com/article/us-china-tech-taxation-idUSKBN28Q10Z (accessed 18 January 2021).

[251] Noonan and Plekhanova, *supra* note 201, 1036.

[252] UK Government, *WTO General Council: UK Statement on Work Programme on Electronic Commerce*, 13 October 2020, available at https://www.gov.uk/government/speeches/uk-statement-to-the-wto-general-council--6 (accessed 17 February 2021).

[253] Williams, 'US Senators Warn UK Digital Services Tax Could Derail Trade Talks', *FT* (2020), available at https://www.ft.com/content/a20bf740-c310-4a90-9dd8-81369cfb1bdc.

[254] A. Seely, *Research Briefing: Digital Services Tax* (2020), available at https://commonslibrary.parliament.uk/research-briefings/cbp-8719/ (accessed 17 February 2021). Note that the UK has said that it will disapply the tax if an appropriate global solution is agreed.

[255] USTR, Section 301 Investigation: Report on the United Kingdom's Digital Services Tax, 13 January 2021.

[256] Hogan Lovells, *Is the DST Compatible with the UK's International Obligations?*, 11 November 2019, available at https://www.hoganlovells.com/en/publications/is-the-dst-compatible-with-the-uks-international-obligations (accessed 1 November 2020).

[257] Lowry, *supra* note 233.

[258] Noonan and Plekhanova, *supra* note 232.

[259] J. P. Meltzer, 'Cybersecurity, Digital Trade, and Data Flows: Re-Thinking a Role for International Trade Rules', *SSRN Electronic Journal* (2020), available at https://www.ssrn.com/abstract=3595175 (accessed 26 October 2020).

[260] As with other aspects of digital trade, there are deficiencies in the ways that current trading rules are drafted. For instance, the WTO security exception is likely too limited in scope for governments to justify many measures taken to prevent economic espionage, cyberattacks on critical infrastructure, or manipulation of online information. *Ibid.*

[261] Other, less high-profile emerging issues include commitments that promote open government data, with Parties endeavouring to ensure that, where they choose to make non-personal or anonymised public sector data available in open, machine-readable formats, it can be searched retrieved, reused, and redistributed (eg see art. DIGIT.15 TCA). The recent Digital Economy Agreement between Australia and Singapore, provides an indication of other emerging issues. It includes commitments on promoting the use of digital identities and development of interoperable approaches (art. 29); co-operation on competition policy to develop and implement approaches to address the challenges of digital markets (art. 15); co-operation on vital digital infrastructure, including commitments to facilitate submarine cable installation, maintenance and repair, and the prevention of cable disruptions (art. 22); co-operation in conformity assessment and digital standard-setting (art. 30); co-operation to develop AI governance frameworks (art. 31); and co-operation on FinTech and RegTech (art. 32).

[262] In the government's impact assessment and analysis of the UK–Japan agreement for instance, there was very little detail on digital trade. See pages 8, 26, Department for International Trade, *supra* note 95; Department for International Trade, *UK, The UK–Japan Comprehensive Economic Partnership Benefits for the UK* (2020), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929065/UK-Japan-Trade-Agreement-sectoral-benefits.pdf (accessed 17 February 2021).

[263] UK Government, *Trade Advisory Groups: Membership* (2020), available at https://www.gov.uk/government/publications/trade-advisory-groups-tags/trade-advisory-groups-membership (accessed 17 February 2021).

[264] E. Jones and A. Sands, *Parliamentary Scrutiny of Trade Deals: How Does the UK Measure Up?*, 30 September 2020, UK Trade Policy Observatory, available at https://blogs.sussex.ac.uk/uktpo/2020/09/ (accessed 21 January 2021); *UK-Japan Comprehensive Economic Partnership Agreement: Second Report of Session 2019–21* (2020), page 5, available at https://publications.parliament.uk/pa/cm5801/cmselect/cmintrade/914/914.pdf (accessed 21 January 2021).