ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

September 25, 2020

EU International Agreements Sub-Committee,

House of Lords,

London, SW1A 0PW

Re: ITIF Written Submission Regarding UK-US Trade

Dear Committee Members,

Please find below the Information Technology and Innovation Foundation's (ITIF) written submission concerning the committee's inquiries into UK-US trade negotiations. It focuses specifically on digital trade issues.

ITIF is a nonprofit, nonpartisan think thank that focuses on the intersection of technological innovation and public policy, including economic issues related to innovation, competitiveness, trade, and globalization; and technology-related issues in the areas of information technology and data, broadband telecommunications, advanced manufacturing, life sciences, agricultural biotechnology, and clean energy. On the strength and influence of this work, the University of Pennsylvania has ranked ITIF as the world's leading think tank for science and technology policy the last two years.

I have written extensively on the issues the committee is focused on as parts of reports and submissions, such as Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?, The False Promise of Data Nationalism, a Submission to New Zealand's Ministry of Foreign Affairs and Trade on Objectives for Digital Economy Partnership Agreement Negotiations, Comments to the U.S. International Trade Commission Regarding the United States-Mexico-Canada Agreement, and Principles and Policies for "Data Free Flow With Trust." These reports and submissions analyze the critical role played by data flows and digital trade and how new trade rules and cooperation are needed to support and protect the role they play in driving economic productivity and innovation.

Sincerely,

Nigel Cory

Associate Director, Trade Policy, The Information Technology and Innovation Foundation

TABLE OF CONTENTS

OUTLINING AN AMBITIOUS DIGITAL TRADE AGENDA FOR THE UNITED KINGDOM

To become a world leader in the global digital economy the United Kingdom needs an ambitious plan to advocate for new rules, norms, and mechanisms for cooperation on digital trade, data governance, and standards related to emerging technologies. It's overarching goal—building rules-based, interoperable, and innovation-friendly approaches at the bilateral and global level. This submission focuses on the International Trade Committee's inquiry into the United Kingdom's engagement and negotiations with the United States. However, each of the policy ideas could be applied to the Committee's inquiries into trade engagement with Australia, Japan, and New Zealand. Together, they also relate to the Committee's broader inquiry into the United Kingdom's future trade policy in outlining a vision for an ambitious post-Brexit digital trade agenda.

From a digital trade perspective, the United Kingdom's sequencing of trade negotiations with these countries is ideal as they all prioritize digital trade. The United Kingdom's public statements on digital trade as being a key benefit of its post-Brexit trade policy reflects its broad alignment. There are also significant economic and digital trade connections between the parties. The United States and United Kingdom are the world's leading exporters of digitally delivered services.[1] According to a PayPal survey (involving 6,000 online consumers across six key markets) of cross-border e-commerce, 70 percent of respondents shopped in the United States, while 47 percent of Australians said they shop in the United Kingdom.[2] These countries also lead the world in pushing for new rules and cooperation around digital trade, data governance, and data-driven innovation for new and emerging technologies.

The UK's review of domestic and trade strategies is an opportunity for the United Kingdom to join its peers in building an open, rules-based, and innovative global digital economy. In this context, the Information Technology and Innovation Foundation (ITIF) has already provided extensive material to UK officials regarding global digital trade policy developments, especially in regard to where the "gold standard" lies in terms of new, binding rules.[3] These new rules protecting data flows and digital trade are much needed given the spread of digital protectionism globally. The Committee has already received submissions and heard testimony outlining the need for a range of specific new digital trade rules. However, that's not the focus of this submission (The exception is the idea for new rules to support the UK's video game sector).

While important, new digital trade rules only get countries so far given how much modern trade involves behind-the-border regulatory and legal issues. Every one of the UK's major trading partners are simultaneously dealing with domestic debates about how to address digital and data-related issues and how to support the development and use of data and emerging technologies, while also trying to work with other countries to support their role in trade. An ambitious outcome should involve both new binding trade rules and cooperation to build interoperable governance of data and digital trade.

This submission provides new ideas about how the United Kingdom should and can do this. In most cases, these actions involve the UK government identifying and building cooperative mechanisms for key enablers of digital trade and innovation. Just as the United Kingdom works with its "Five Eyes" partners (Australia, Canada, New Zealand, and the United States) to standardize operating practices and technical specifications for defense equipment and operations, it should seek to build out a trade and innovation framework. It

should also do this with other similarly ambitious countries like Chile, Japan, and Singapore. It should obviously explore joining the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). If the United Kingdom wants to truly maximize the benefits of digital trade and technologies, it needs to proactively pursue rules around transparency and good regulatory practices and develop mechanisms for cooperation on data, emerging technologies, and standards with the same determination it gives to pursuing lower tariffs for agricultural and manufactured goods.

CONCEPTUALIZING A SUCCESSFUL DIGITAL TRADE STRATEGY

Digital trade provisions and cooperation are an economic multiplier as they support broader, dynamic economic and trade activity. It's an effort to achieve an outcome that is more than the immediate and directly quantifiable sum of its parts. This can make it hard for policymakers to rally around. An ambitious UK digital trade agenda is not as easy for elected officials and policymakers to explain to local constituents. It can be hard to explain how a new rule to ensure the flow of personal and other data (which a firm may already take as a given) is continued thanks to new trade rules that prohibit new restrictions. Likewise, it can be difficult to explain how new rules and cooperation ensure a firm can seamlessly—using the same tech tools and financial and payment arrangements—work with a partner they never physically meet on a deal involving digital content delivered over the Internet to customer in a third country.

Digital trade advocacy also doesn't lend itself to the economic calculations involved in the econometric modeling traditionally used to assess the success of trade agreements. While it is hard to draw a direct link with some shift in gross domestic product, the digitalization of the economy means it'll indirectly appear as it supports the development and adoption of digital tools that improve economic productivity and firm competitiveness and innovation. The future of domestic economic competitiveness and international trade increasingly resides in services, data, and knowledge—all of which are affected by the behind-the-border measures targeted by an ambitious digital trade agenda.

To this end, the UK's strategic objective should be to develop an open, rules-based, and innovative global digital economy. This goal stands in direct competition with the other two main models for digital development and governance: the restrictive European Union (EU) model and the sovereignty, surveillance, and control-focused Chinese model. Modern technology, especially the Internet and cloud data storage, means that each country's domestic regulatory regime for data (such as for privacy) needs to be globally interoperable as each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions. In this way, the Internet means digital technologies create interdependences between regulatory regimes. But both the EU and China fail to recognize these central points and instead enact artificial, geographic and other restrictions on the transfer of data in a misguided and damaging effort to try and control the Internet.

Instead, the UK should place interoperability at the heart of its model. It's a better model for global Internet governance as it recognizes and allows data to flow between different regulatory regimes on the global Internet, while ensuring a countries' data protection rules flow with it. Firms are held accountable for how they manage data, regardless of where they transfer and store it.[4] Interoperability is already at the heart of

many countries' data protection frameworks and internationally agreed privacy principles (such as those from the Organization for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC)). But it needs greater, explicit support from the United Kingdom and others.

The global digital economy urgently needs more digital free trade champions, especially amidst a global pandemic where digital services are now essential. Digital trade barriers are not widespread in the United Kingdom's first set of negotiating countries. However, ambitious digital trade outcomes in these agreements would build new global rules and norms that counter those barriers to trade enacted by China, Russia, the European Union, and others. This is central to the contest between the different models of data governance and digital development.

Success will depend on whether the United Kingdom and likeminded digital trade allies can work with and persuade the many undecided countries in the middle—those that have not yet chosen a particular model to follow—that their model is the best from both an economic and regulatory perspective. This submission's ideas will hopefully make the UK's innovative and digital trade-friendly model more successful, thus appealing to other countries and thus helping its chances of becoming the global norm.

NOT JUST THE TEXT: USING COOPERATION TO BUILD BETTER GOVERNANCE AND TRADE IN DATA, DIGITAL CONTENT, AND NEW AND EMERGING TECHNOLOGIES

Usually, international cooperation and trade rules follow well after each country's domestic debate around new laws and regulations for new and emerging technologies. New digital trade rules are definitely needed to prohibit and roll-back the growing range of barriers, but these are insufficient on their own to future-proof (as much as possible) trade frameworks so that firms can engage in seamless cross-border digital trade and innovation.[5] The pace of innovation and competition for every possible advantage in the global battle for tech leadership means UK trade policy also needs to be dynamic. If the United Kingdom wants to create a truly innovation- and digital trade-friendly framework, UK policymakers must build cooperation with likeminded trading partners to ensure the early and ongoing alignment in how they govern data and new digital technologies.

Cooperation at the early stage of discussions around data and digital issues can hopefully lead to the sharing of information about how to best address them, while also avoiding policies that act as barriers to digital trade and data-driven innovation. This could cover data privacy, digital identity, payments, artificial intelligence (AI) governance, or some other issue. Such international cooperation shouldn't be left as an afterthought for years after a policy comes into effect. Unfortunately, this is China and the European Union's approach to privacy, data flows, cybersecurity, and artificial intelligence, which means they become country- and region-specific barriers to digital trade.[6] It's much harder to retrospectively change or work around these regulatory differences. Nor should such cooperation be left to multilateral forums, given it'll likely be held back by the member with the lowest level of ambition or interest. Therefore, the United Kingdom should build cooperation with its allies to build shared, interoperable outcomes with its likeminded trading partners on digital- and data-related issues.

Australia, Chile, New Zealand, and Singapore show how this is done through their respective digital economy agreements. These agreements often don't include new binding trade rules, but instead use MOUs and agreements to cooperate on data innovation, AI, data portability, e-payments, e-invoicing, e-certification, trade facilitation, data privacy, the Internet of Things, blockchain, smart cities, and digital identity issues.[7] These four countries are using these digital economy agreements and MOUs to ensure the regulation of these digital trade enablers are aligned. It allows the various partners to build a better understanding about respective approaches to new issues and to provide confidence and clarity around current arrangements and a connection between regulators as rules and technology change. The end goal is to ensure their respective approaches are interoperable—thus ensuring firms are able to work as seamlessly as possible across borders in conducting digital trade.

These digital economy agreements show how truly modern trade agreements are as much about pursuing a model for digital governance that is international and interoperable as it is about agreeing on new, binding trade law provisions.[8] It reflects a holistic approach in addressing both existing barriers while also working together to prevent new ones emerging as part of changing domestic laws and regulations. As Ravi Menon, Managing Director, Monetary Authority of Singapore (MAS), has stated, in the digital economy of the future data connectivity agreements among countries will become as important as today's free trade agreements. The United Kingdom would do well to follow this approach.[9]

Besides trying to prevent future barriers, binding trade law commitments could also apply better regulatory policies to existing practices that may act as a barrier to digital trade. For example, the U.S.-Mexico-Canada trade agreement (USMCA) includes a new "good regulatory practices" chapter—the first of its kind for a U.S. trade agreement—which aims to reduce and prevent non-tariff barriers through increased transparency, evidence-based decision-making, and whole-of-government internal coordination.[10] Chapter-specific commitments on cybersecurity (article 19.15) and Internet-based value-added services (like platforms, article 18.14) apply the same requirements to these digital trade related goods and services.[11]

Besides commitments on good regulatory practices, the United Kingdom should use MOUs to build a framework for cooperation between regulatory agencies involved in data and emerging technologies. Privacy, financial oversight, and other digital-related regulators may already have MOUs or international meetings, but due to a variety of reasons—such as a lack of capacity and resources, concerns that trade officials are infringing on their regulatory sovereignty, and the general perception that they're domestic, not international, agencies—they haven't updated, prioritized, or pursued closer engagement and cooperation with foreign counterparts. Where necessary, UK policymakers should ensure the country's digital- and data-related regulators are engaged internationally.

For example, Singapore is leading the way in how its central bank (MAS) is pursuing agency-to-agency fintech MOUs with key counterparts in Australia, the United Kingdom, and the United States in order to support cross-border data flows, innovation, and digital trade in the sector. At the heart of these MOUs lies the recognition that however fintech evolves, the free flow of data and regulatory access to it will remain critically important to trade and innovation. The U.S. Department of Treasury is also heading in the right direction in agreeing to a MOU with MAS and flagging its interest in the issue more broadly.[12]

Regulatory cooperation around MOUs would ensure respective agencies share information at the earliest stages of the rulemaking process. It would also hopefully give other countries' governments and firms a seat at the table or ability to contribute feedback. Ultimately, it'd hopefully allow regulators to discuss issues, options, and ways to identify and eliminate differences in regulations—all in the shared interest of facilitating effective policy, and also trade and innovation.

Cooperation on enforcement—such as on shared privacy, cybersecurity, and financial oversight issues—should be part of greater regulatory cooperation. The United Kingdom has taken many steps in the right direction here, but more could be done. For example, on March 5, 2020, the UK's Information Commissioner's Office (ICO) and Australia's Information Commissioner signed an MOU to share information and best practices and to cooperate on specific projects and investigations. Following this, on July 9, Australian and British privacy regulators opened a joint probe into Clearview AI in order to examine how the company's facial recognition technology uses people's data.[13] Similarly, the ICO already has an MOU with New Zealand (on spam emails), the U.S. Federal Trade Commission, and Canada's Office of the Privacy Commissioner.[14] These should be reviewed to ensure they cover the full spectrum of issues and provide a productive mechanism for information sharing, cooperation, and joint enforcement. Building better connections between enforcement agencies builds trust and confidence in domestic regulatory agencies that digital trade agreements and cooperation can help, not hinder, their ability to do their jobs.

MOUs and cooperative arrangements are a dime-a-dozen in trade agreements and economic statecraft. The only thing that makes them valuable is if the parties find them useful. Australia, Chile, New Zealand, and Singapore show this is clearly possible between small groups of countries that are similarly ambitious about digital trade and data-driven innovation. Trade agreements have long included "soft" commitments for parties to cooperate on certain issues, but with digital technologies emerging as a key driver of trade and innovation and behind-the-border regulations having a growing impact on trade, these commitments can no longer represent meaningless gestures where parties simply put issues they couldn't agree on (as a sort of "too-hard" basket) or where hard, binding rules didn't seem to fit. For the United Kingdom to become a leader in the global digital economy, it needs to change this and push for new and meaningful cooperation and regulatory alignment on key enablers of digital trade and data-driven innovation.

Open Data and Data Trusts: Unlocking Public and Private Data for Digital Trade and Data-Driven Innovation

As the United Kingdom and its trading partners pursue national strategies to increase their competitiveness in AI, including via digital trade, they should use data trusts and other data-sharing models to improve the quality (and the quantity) of the data that is the key input into digital goods and services. This matters because AI needs good data, not just more data.[15] For example, in a survey of 179 data scientists, over half identified addressing issues related to data quality as the biggest bottleneck in successful AI projects.[16] Therefore, it makes sense for the United Kingdom to use digital trade commitments to encourage others to adopt open data frameworks for public data and data trusts and other models for the voluntary sharing of high-quality data.

"Open data" refers to data that is made freely available without restrictions.[17] Many governments have begun to embrace open data to encourage transparency and accountability, increase public participation, and promote economic growth. In many cases where high-quality data exists, it is dramatically underutilized. To this end, the United States is working through mechanisms to improve public-private data sharing.[18] As of 2018, the United Kingdom ranked 52nd out of 178 in the Open Data Inventory (ODIN)'s global index (of open data regimes for national statistical offices).[19] The United Kingdom should be commended for its National Data Strategy, which seeks to expand data trusts within government.[20] The United Kingdom recognizes open data is a key barrier to better AI and is already trying to develop a model for "data trusts" to overcome.[21]

However, government data is only a fraction of the data that could be useful for AI development. For example, many major pharmaceutical companies have begun sharing historical clinical trial data with outside researchers, including competitors. Benefits include faster drug development, a better understanding of diseases, and more efficient clinical trials.[22] However, many stakeholders lack the mechanisms to share data while ensuring the protection of this proprietary and sensitive data. This highlights the government's role in identifying opportunities at home and abroad (with trade partners) to encourage the development and use of open data frameworks. If governments don't take on this coordinating role in identifying, developing, and supporting these data-sharing models, it is unlikely that organizations in many sectors will create them on their own.

To be clear, these data-sharing initiatives should be voluntary and should not involve compulsory data sharing. Only in cases where there is a clear market failure and firms control particular datasets for which they strictly limit access, should governments step in. Such a situation exists in the real estate and air travel industries in the United States.[23] Forcing companies to give up valuable data they have spent considerable time and money collecting and using to competes makes no more sense than forcing them to give up valuable patents, trade secrets, employees, or property.[24] It would undoubtably boost competitors, but it would also degrade business's incentive to make future investments in these areas.

The United Kingdom should push for a specific open data section in its digital trade agreements, starting with the general recognition that opening up public information for re-use has considerable and widespread benefits to government, industry, and the public. The United Kingdom should require parties to have an open-by-default framework for government data in place (without being prescriptive, as each country will approach the issue in their own way) and demand trading partners should adhere to best practices for open data, including ensuring it is published in open, machine-readable formats. Given the need to avoid prescriptive frameworks, the United Kingdom should explicitly reference international agreements that signal that a country is committed to enacting best practices, such as the G8 Open Data Charter and the Open Government Declaration (both of which the United Kingdom has signed on to).[25]

The United Kingdom could also use MOUs and cooperative arrangements with trading partners to identify opportunities to build data-sharing frameworks between stakeholders in different countries. This could lead to sector-specific data trusts. For example, the Digital Catapult in the United Kingdom plans to publish model agreements for start-ups entering into data-sharing agreements.[26] The United Kingdom could connect this

model with similar programs in other countries. Doing so would support the development of better physical and digital products and services. These datasets would be particularly useful for startup or other small organizations that do not have access to significant amounts of data.

Building Collaboration on Emerging Technologies: High-Performance Computing and Advanced Manufacturing

Nations are fiercely competing for manufacturing leadership, including through the development and use of high-performance computing (HPC) systems and other digital tools. Countries should develop national manufacturing digitalization strategies to support the broader development and use of these technologies.[27] However, if they wish to give their firms the best possible support they should also connect centers of excellence and relevant firms with their international counterparts to share best practices and to build trade connections.

Small manufacturers, especially, can't be expected to go-it-alone in this environment and will need help from their government to establish collaborations with foreign partners and centers of excellence. In this context, the government can use trade and economic engagement to connect academic, public, and private sector representatives in the United Kingdom and their trading partners to identify opportunities for industrial collaboration on new and emerging technologies.

The United Kingdom needs to target these technologies as they're central to future trade competitiveness in advanced manufacturers. ITIF's report "Why Manufacturing Digitalization Matters and How Countries Are Supporting It" explains how digitalization is transforming manufacturing globally, detailing what exactly smart manufacturing is and examining the productivity impacts that digitalized manufacturing promises to deliver.[28] Whether it's called "Industry 4.0," as in Europe, the "Industrial Internet of Things (IIoT)," as in the United States, or simply "smart manufacturing," the application of information and communication technology (ICT) to every facet of manufacturing is in the midst of reshaping modern manufacturing, and thus, trade in manufactured goods.[29] Smart manufacturing is being driven by the advent and maturation of many technologies, including: HPC-powered computer-aided design (CAD) and engineering (CAE) software; cloud computing; the Internet of Things; advanced sensor technologies; 3D printing; industrial robotics; data analytics; machine learning; and wireless connectivity that better enables machine-to-machine (M2M) communications.

Digital aspects of advanced manufacturing, such as HPC, deserve special attention within the United Kingdom as its domestic productivity lags well behind global leaders. UK manufacturing has suffered low levels of productivity for decades—the Office of National Statistics reported that the productivity gap to other G7 countries in 2016 was 16.4 percent.[30] Moreover, a recent UK Innovation Survey found that just over half of UK businesses are classified as innovative and that fewer UK small and medium-sized enterprises (SMEs) introduce new products and services than their European competitors.[31]

However, the United Kingdom is not alone in battling low levels of productivity in the manufacturing sector. U.S. manufacturing productivity grew just 1 percent from 2011 to 2016, the lowest recorded rate since 1948

(when the statistic was first measured). Even in Germany, which introduced the term Industry 4.0 into the lexicon, a 2015 survey of 4,500 German SME manufacturers found that less than 20 percent had even heard of Industry 4.0, much less taken steps to implement it.[32] Likewise, a June 2017 survey of 250 U.S. SME manufacturers found 77 percent reporting that they still had no plans to implement IIoT technologies.[33] Given this shared challenge, UK trading partners may be interested in creating new ways to work together on HPC and advanced manufacturing.

The United Kingdom should use cooperation on defense-related research as a model to replicate for advanced manufacturing and the use of emerging technologies such as HPC. For example, on defense science and technology, the Five Eyes Technical Cooperation Program already involves many collaborative research and information exchanges, including on new and emerging technologies such as autonomy, the electromagnetic spectrum, advanced manufacturing, and urban environments.[34] In 2017, the United States added the United Kingdom (and Australia), to the National Technology and Industrial Base (a legal framework previously limited to the United States and Canada) to create new opportunities for joint R&D and controlled technology transfers.[35] Early "Pathfinder" projects are already underway exploring how this will open new avenues for cooperation involving the United States, Canada, Australia, and the United Kingdom.[36]

UK-U.S. cooperation on defense-related research is even broader. In 2018, there were around 220 formal science and technology collaboration agreements between the United States and the United Kingdom.[37] Across the breadth of all UK academic research, approximately 10 percent is performed collaboratively with U.S. universities and approximately 20 to 25 percent of all defense science and technology R&D in the United Kingdom is carried out collaboratively with U.S. partners.[38]

It will take a concerted, considered effort for the United Kingdom to replicate this type of cooperation for key emerging technologies with similarly ambitious and interested trading partners, whether it comes to Australia, Japan, or elsewhere. It's also a matter of identifying where trading partners prioritize the same technologies and where there are gaps in existing forums and agreements. The United Kingdom already has many key pieces in place to do this with the United States.

In September 2017, the United Kingdom and the United States signed the first-ever Science and Technology Agreement, which commits both nations to strengthening collaboration on research, science, and innovation.[39] The agreement sets out core agreements on the treatment of intellectual property, the confidentiality of data, and export controls.[40] It does not specifically mention advanced manufacturing or high-performance computing. However, in 2018, the U.S. Lawrence Livermore National Laboratory (LLNL) and the UK's governing body for scientific research signed a new three-year agreement to improve U.S. and UK industries through better use of high-performance computing, research collaboration, and joint economic promotion.[41]

The United Kingdom should bring the various parts together and connect it with each country's respective strategies to support advanced manufacturing at home. The United Kingdom should use trade-related cooperation on advanced manufacturing as the international extension of its domestic "sector deals," innovation hubs, and its High-Value Manufacturing Catapult (HVMC). The November 2017 report by the

UK's Department for Business, Energy, and Industrial Strategy (BEIS), *Industrial Strategy: Building a Britain Fit for The Future*, proposed the establishment of these "sector deals." In the proposal, individual sectors come together under clear leadership to negotiate sector-specific deals with the government to boost the sector's earning power and productivity. The Industrial Strategy announced several completed "sector deals" focused on industrial digitalization and AI in the automotive, life sciences, construction, and creative industries.[42] Furthermore, the *Made Smarter* review called on the United Kingdom to create twelve "digital innovation hubs," eight large-scale demonstrators, and five digital research centers focused on developing new technologies as part of the new National Innovation Programme.[43]

The United Kingdom's network of ten Catapult Centers—not-for-profit, independent, physical centers that focus on the commercialization of new and emerging technologies and that connect businesses with the UK's research and academic communities—would be central to new cooperative arrangements with the United States and other trading partners.[44] In particular, the HVMC, which is comprised of seven individual centers, facilitates the application of leading-edge technical knowledge and expertise to the creation of products, production processes, and associated services that have strong potential to bring sustainable growth and high economic value to the UK. The seven HVMC centers have capabilities and competencies that span basic raw materials through to high-integrity product assembly processes.

The seven HVMC centers include: the Advanced Forming Research Centre; the Advanced Manufacturing Research Center; the Centre for Process Innovation; the Manufacturing Technology Centre; the National Composites Centre; the Nuclear AMRC; and the WMG Catapult.[45] Analysts regard the HVMC as a particular success, as since its inception in 2012, it has tripled the impact of government spending, generating £655 million of additional income from the industry by working with over 3,000 businesses every year to bring new technologies to market.[46] The Catapults work with manufacturing businesses of all sizes (though in practice it's often challenging to engage SMEs), providing them access to leading-edge equipment, expertise, and an environment of collaborative innovation.[47]

The United Kingdom could explore how to use current trade negotiations and economic engagement to deepen linkages between its Catapults and America's Manufacturing USA network, Australia's Entrepreneurs Program, and Japan's Industrial Value Chains Initiative (IVI) and its Cross-Ministerial Strategic Innovation Promotion Program focused on Innovative Design/Manufacturing Technologies. As to the former, Manufacturing USA consists of 15 manufacturing innovation institutes representing public-private partnerships. They focus on developing advanced manufacturing product and process technologies, facilitating their commercialization, and developing workforce skills around advanced manufacturing technologies.[48] Manufacturing USA plays a pivotal role in revitalizing the U.S.'s industrial competitiveness and ensuring U.S. leadership across a range of advanced-manufacturing processes and technologies.[49]

At least four Institutes of Manufacturing Innovation (IMIs) within Manufacturing USA address smart manufacturing-related technologies and processes. The first IMI, America Makes: The National Additive Manufacturing Innovation Institute, launched in 2011, focuses on expanding manufacturers' additive manufacturing (i.e., 3D printing) capabilities. The Digital Manufacturing and Design Innovation Institute (since renamed MxD) encourages factories across America to deploy digital manufacturing and design

technologies, so America's factories can become more efficient and cost competitive.[50] The Institute for Advanced Composites Manufacturing Innovation (IACMI) accelerates the development and adoption of cutting-edge manufacturing technologies for low-cost, energy-efficient manufacturing of advanced polymer composites for vehicles, wind turbines, and compressed gas storage.[51] Finally, the Clean Energy Smart Manufacturing Innovation Institute (CESMII) focuses on innovations such as smart sensors, data analytics, and controls in manufacturing that can dramatically reduce energy expenses in advanced manufacturing.[52]

Cooperation and engagement between the United Kingdom and its trade partners on HPC and advanced manufacturing won't lead to new binding rules. Instead, it'll build the framework to connect relevant policymakers and private-sector representatives to discuss, develop, and share best practices and connect firms that may be interested in working together on trade and research opportunities. It may take the form of government-to-government, agency-to-agency, or public/private MOUs that outline shared interests, principles, and best endeavors to consistently and proactively work together on shared public policy issues and in facilitating private sector connections. This project could eventually evolve into formal exchanges and secondments between respective programs. This would be in line with the use of MOUs on AI, data privacy, digital identity, and other digital issues between Australia, Chile, New Zealand, and Singapore in their recent digital economy partnership agreements.[53]

It would be worth exploring whether the United Kingdom and its partners could identify other issues to establish a cooperative framework through trade policy to connect firms involved in HPC, such as environmental science, life sciences, and more. For example, for high-performance computing, the global COVID-19 HPC Consortium manages a range of computing capabilities that span from small clusters to some of the largest supercomputers in the world. The UK Digital Research Infrastructure is a member, becoming the first member with a supercomputer in Europe, joining IBM and the U.S. Department of Energy, which are co-leading the effort.[54] The contribution will involve facilities across the country, including the Engineering and Physical Sciences Research Council's ARCHER supercomputer at the University of Edinburgh, the Science and Technology Facilities Council (STFC) supercomputing facilities, DiRAC and the Hartree Centre at Daresbury Laboratory, and the Biotechnology and Biological Sciences Research Council's (BBSRC) Earlham Institute.

Building Pre-Standardization Cooperation for New and Emerging Digital Technologies

The Committee's questions show it recognizes the important role standards play in modern trade. Identifying how to make existing standards and regulatory systems compatible between different regimes is a legitimate, but complicated, debate and process. However, there is also room for creative cooperation on standards for new and emerging technologies that is beyond the scope of traditional standards issues (such as mutual recognition). The United Kingdom should pursue pre-standardization cooperation as part of, and alongside, its trade agreements to ensure its technology firms have the advantage of basing their technology on the same foundational, technical elements (in terms of terminology, measurement methodology, and other technical processes) as other leading tech-driven trading partners, such as Australia, Japan, and the United States. All of

this can be done well before standards are finalized and part of regulatory systems that are much harder to change once enacted.

Standards define some specific characteristics for a specific item (which may be, for instance, a material, a product, a procedure, a process, or a service), to make such an item meet certain well-defined objectives (which may relate, for instance, to performance or interoperability).[55] Standards can be physical, reference material, a measurement protocol, documentary standard, a technical specification, a guidance document, or a best practice. Standards development work is a collaborative activity that engages a wide array of subject matter experts from the private and public sectors including industry, government, academia, and standards development organizations (SDOs).[56]

Standards are a key tool in the global race for innovation and trade advantage in new and emerging technologies, whether it's 5G, AI, data privacy, facial recognition, advanced manufacturing, digital finance, or other sectors. Given their role, there are two faces to the standards coin: cooperation and collaboration vs. competition. However, with similarly ambitious, tech-focused, and value-sharing partners, the former can be important for firms from both parties to help them compete, especially against firms from other countries or regions that use restrictive standards.

Divergent standards are often an obstacle to spreading technologies and hamper interconnection and interoperability. Even worse, they can impede the development and deployment of new technologies if stakeholders don't coalesce around one widely agreed upon approach. For example, it may lead to reduced or hedged investments across new and emerging technologies as tech firms (and investors) wait and see which standard prevails as the dominant one. Standards unique to a country (such as China) or region (such as the European Union) make it more difficult and costlier for foreign firms and their products to be sold in those markets as they need to reconfigure preexisting design and production processes to suit those specific standards, and pay royalty fees for providing products using the local standard. This disrupts the global, generally standardized production processes on which many foreign companies rely on to compete.

China provides a clear example of how country-specific standards can act as a barrier to trade for high-tech goods and services.[57] As ITIF's report "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" argues, China has made the development of indigenous technology standards, particularly for ICT products, a core component of its industrial development strategy.[58] Similarly, Richard Suttmeier's "A New Technonationalism?: China and the Development of Technical Standards" details the early 2000s battle over China's efforts to promote its own wireless communications standard WAPI (wireless authentication and privacy infrastructure).[59]

Most recently, in 2018, China introduced a new standardization law that will likely favor local firms and goods and services, as it references "indigenous innovation" while failing to reference either its WTO commitments (therefore raising questions about WTO compliance) or its acceptance of existing international standards (as approved by the various SDOs).[60] Indicative of China's approach, a report by the German think tank Mercator Institute for China Studies (MERICS) shows Chinese standards for basic smart manufacturing correlate with about 70 percent of relevant international standards—which falls to around 53 percent for key

smart manufacturing technology standards, and to 0 percent for standards relating to cloud computing, industrial software, and big data.[61] China pursues indigenous (i.e., China-specific) technology standards because it believes it will advantage China's domestic producers while blocking foreign competitors and reducing the royalties Chinese firms pay for foreign technologies.[62]

The United Kingdom clearly recognizes the role and value of international standards: 85 percent of British Standards are developed in international and European processes.[63] While the United Kingdom and its national standards body (BSI) have long been engaged in European and international standards bodies, the challenge to prosecute this in the future will get more difficult after Brexit. It can't bank on its partners in Europe and the European Union adopting an approach that best suits its objectives as it relates to new and emerging technology. China is also fast emerging as a major player in international standards, which is potentially concerning given it takes a different and restrictive approach to standards at home.[64] The United Kingdom should review its current approach and consider how it'll deal with digital standards after Brexit—both within its trade agreements, but also parallel to it.[65]

Pre-standardization cooperation is a creative, forward-looking way for the United Kingdom to work with likeminded partners on the early alignment of key terminology and concepts, technical details, and policy discussions. There are existing forums and cases to show the value of pre-standardization cooperation on new and emerging technologies. For example, in 1982, regulatory agencies and laboratories from G8 countries (now the G7) and the EU came together as part of the Versailles Project on Advanced Materials and Standards (VAMAS) to develop standardized terminology, reference materials, and testing and measurement protocols for new materials (physical, chemical, material, electronics etc.).[66]

As part of the inter-laboratory testing (also referred to as round robin testing) processes, VAMAS stakeholders sent samples to multiple labs to test draft protocols they'd developed to see if the results from different participating laboratories got the same results and to identify where the protocol didn't work and how to correct it. VAMAS stakeholders had an MOU with the International Organization for Standardization (ISO) to help feed their pre-standardization cooperation into the formal standards-making process.[67] This MOU has greatly benefited both organizations, as is evident by the strong cooperation between VAMAS Technical Working Areas addressing nanotechnology-related measurements and the ISO Technical Committee 229 (Nanotechnologies), which is chaired and supported by BSI. VAMAS continues to work on a range of physical materials, with an expanded membership, including Brazil, Mexico, South Africa, Australia, India, and China.[68] Its work was (and remains) immensely useful as it allows the final, consensus standards to be based on the same terminology and measurement and testing procedures.

Other examples of pre-standardization work involve researchers from Germany, Japan, and the United States working together on electrokinetic measurements and quantification of coarse particle content (such as those uses in advanced materials, thermal coatings, and drug carriers).[69] Another example involves standards-related collaboration between the U.S. National Institute of Standards and Technology's (NIST) and the European Commission's Joint Research Center (ECJRC) for the development of reference materials for nanotechnology and health-related measurement standards.[70] Another recent example involves nanomaterials and measuring toxicity at the nanoscale.[71]

Pre-standardization cooperation is a technical and scientific, not political, process. Given standards are a key part of the battle for innovation advantage between the United States, China, the EU, and others, it can be much harder to cooperate and coordinate on standards for more mature technologies as they become increasingly tied to political objectives, built up infrastructure, sunk investment costs, and enacted (and thus hard to change) laws and regulations. For firms and other stakeholders, pre-standardization work can be easier than final-stage formal standards development as they're not already heavily invested in existing standards guidance. Trying to change standards for mature technologies can be problematic given the cost and complexity involved in ensuring future and backward supply compatibility (i.e., retooling design and production processes to suit a new standard). This is why pre-standardization cooperation could be a more pragmatic objective for standards cooperation as it is technically focused and done at the early stages of technological innovation, before potential uses and outcomes have been politicized or broadly adopted and deployed by firms.

The United Kingdom should work with trade partners and their stakeholders (those involved in technology standards, whether from government, academia, or the private sector) to identify opportunities for closer, more active cooperation on pre-standardization discussions for new and emerging technologies. Such collaboration should be driven by the goal of helping support scientific discovery—rather than simply fulfilling a politically driven commitment made in a trade agreement. It'd ensure their respective stakeholders are engaged with likeminded partners at the earliest stages of technological innovation in discussing and working toward common foundational elements for potential future standards. It could involve identifying use cases for the technology at the heart of the standards process and associated ethical, societal, and governance concerns.

For firms and other stakeholders engaged in cutting-edge research, such early-stage cooperation gives them an opportunity to inform discussions, learn from peers, and help inform potential standards and policy objectives. Pre-standardization cooperation also accelerates the formal standards development process. Standards that are informed by these pre-standardization efforts would obviously benefit participants given it'd align with their products and processes. So even if, for whatever reason, countries created and adopted different standards on the same product, they at least would have a common foundation, which inevitably means there would be considerable similarities. For firms, this reduces the cost and complexity of using the different standards in products developed for multiple markets, which is where significantly different standards become a barrier to trade.

These general outcomes could be flagged in a pre-standardization section of UK trade agreements. There may be existing fora or agreements that parties could revise through better direction, support, and coordination from respective governments and stakeholders. But in cases where existing forums or agreements don't exist or are insufficient, the United Kingdom and its trade partners (and relevant stakeholders) could use formal MOUs to create a framework for pre-standardization cooperation.[72]

The UK has many centers of excellence that could contribute to such an effort on pre-standardization cooperation. BSI is already engaged in developing and advocating for new standards on emerging technologies at home and at international bodies.[73] Unfortunately, NIST's UK counterpart—the National Physical

Laboratory (NPL)—was a major driver in the VAMAS project, but it has become increasingly disconnected from it and has mostly walked away from any leadership responsibilities in the project (though NPL staff are still active in various VAMAS projects). Hopefully this doesn't reflect on, or impact, the UK's interest and ability to engage with others on pre-standardization issues and that other government agencies and non-government stakeholders can step up, such as the Alan Turing Institute and the Centre for Data Ethics and Innovation.

The United States should be a key partner for the United Kingdom on pre-standardization and broader cooperation on standards for new and emerging technologies. For example, the two countries signed a new mutual recognition agreement (MRA, signed in 2019) to replace the MRA between the U.S.-EU Telecom MRA, which means both sides recognize their respective conformity assessment bodies (which relates to standards).[74] A first step would be for the United Kingdom to map existing agreements, fora, and coordination mechanisms and identify gaps and areas for pre-standardization cooperation. For example, BSI and the Institute of Electrical and Electronics Engineers (IEEE, a U.S.-based standards organization) have already set up the Open Community for Ethics in Autonomous and Intelligent Systems (OCEANIS) initiative with other leading standards bodies around the world.[75]

The United States has built a framework that could be used for a more-targeted, active approach to pre-standardization cooperation on new and emerging technologies. In particular, the Trump Administration's Executive Order on Maintaining American Leadership in Artificial Intelligence tasks NIST with developing a plan for federal engagement in the development of technical standards (including international standards) and related tools in support of reliable, robust, and trustworthy systems that use AI technologies.[76] NIST has released a plan for the development of standards for artificial intelligence, including the goal to work with likeminded countries on development of AI standards and related tools.[77] Together, this framework and strategy provides a platform for NIST and other U.S. agencies to potentially work with their UK counterparts to identify shared priorities in standards for new and emerging technology.

The United Kingdom could focus on a range of data and digital-related issues in pursuing pre-standardization cooperation with the United States and other likeminded trade partners. NIST has already done a range of work that could form the basis for a broader agenda to work together on digital and data-related pre-standardization discussions. Indicative of the strong relationship and shared interests, there's already considerable alignment between the United States and United Kingdom on cybersecurity standards. NIST has led efforts to develop globally accepted standards, guidelines, and practices and to advocate for its Framework for Improving Critical Infrastructure Cybersecurity—seen by many as the global standard of best practices for cybersecurity.[78] Since its publication in 2014, the Framework has been updated, translated into various languages, and adapted by government and industries across the globe.[79] NIST has had an active engagement strategy.[80] The UK has introduced several corresponding pieces of law which mirror the framework, including its minimum cybersecurity standard and networks and information security directive.[81] This is indicative of the potential for greater UK-U.S. collaboration and cooperation.

But this should be expanded to other areas, including Internet-of-Things (IoT) systems and devices, and data-related issues. The development of AI standards—particularly technical standards—is at a very early stage in

both countries and elsewhere around the world. For example, most national AI strategies refer to the development of standards for ethical and trustworthy AI. But technical standards to support this goal are still in early stages of development. The United States is trying to fill this gap. It'd be beneficial to UK firms and stakeholders to be involved to ensure they able to inform and align their technology with the U.S. process, given it'll shape a large part of the global market. Likewise, U.S. stakeholders would benefit by feeding into UK thinking around standards and regulation.

The United Kingdom could collaborate with NIST and others on establishing a framework to characterize and measure the trustworthiness of AI systems. For example, terms like "algorithmic transparency" and "algorithmic bias" do not yet have a technical definition.[82] Moreover, the UK and the United States could collaborate on building and using common datasets to develop and test measurement and testing protocols. These programs would provide AI developers in the United Kingdom and United States (and other key trading partners like Australia, Canada, Japan, and New Zealand) with useful guidelines for designing and testing AI systems, allow for the comparison of AI systems, and inform future legislation and regulatory actions.[83] Getting this guidance in the early stages of technological development would help UK researchers developing cutting-edge products as it'd ensure they're broadly in line with future regulatory and legal requirements.

The United Kingdom could also work with NIST and others to develop shared, representative datasets of faces to serve as a more reliable resource for organizations developing facial recognition technology.[84] It could involve best practices for producing explanations or justifications of decisions made by AI systems.[85] NIST is working on both these issues (including via workshops) in a domestic context.[86]

The United Kingdom and its trade partners could also ensure that their respective stakeholders have conducted a technology trend assessment as part of pre-standardization cooperation. For new and emerging technologies at the very early stages of technological development, such assessments highlight certain aspects of a new technology that might conceivably become an area for standardization work in the near-to-medium term.[87] For example, a 2019 proposal at the International Telecommunication Union (ITU) for pre-standardization work on quantum information technology included the evolution and applications of quantum information technology for networks, terminology, and use cases; mapping connections and impact on existing standards and terminology; and identifying its relationship to existing standards and standards-setting forums (so as to avoid duplicative work).[88] Close cooperation between the US, UK, and the European Commission made sure this work was properly scoped and within the expertise of ITU's Telecommunication Standardization Sector (known as ITU-T).

NOT JUST A GAME: PURSUING TRADE RULES TO HELP THE UK'S GAMING SECTOR

The UK's video games industry is the largest in Europe, supporting tens of thousands of jobs. It's a fast-growing sector both domestically and globally.[89] Due to COVID-19, record numbers of people have downloaded games for console, smartphones, and computers. In 2018, games represented 50 percent of the UK entertainment market, and for the first time, outsold music and video combined.[90] As of June 2018, there were 2,261 active game companies in the UK working on e-sports, mobile, PC, and console games and virtual

reality and augmented reality games. The United Kingdom is home to world-class development studios like Rockstar Games, which, with Grand Theft Auto V, developed the most financially successful media product of all time, selling over 95 million units and earning over $6 billion in global revenue.[91] Rocksteady Studios and Ninja Theory are other success stories.[92] Digital trade is critical to this sector—UK games companies generate 75 percent of their revenue from international sales.[93]

The United Kingdom needs to ensure that its video game firms and products do not face opaque, arbitrary, restrictive, and discriminatory content review processes that act as barriers to market entry—like they do in China. In trying to design an ambitious and comprehensive digital trade strategy, the United Kingdom needs to reflect the worst policies that exist, and in many cases, these come from China. As ITIF details in its written submission to a U.S. Senate hearing on "Censorship as a Non-Tariff Barrier to Trade," China is a world leader in digital protectionism and in using censorship and content moderation concerns in broad, discriminatory, and restrictive ways.[94]

Having transparent and predictable access to China's video games market would be a huge win for the United Kingdom's video games sector, as it overtook the United States as the world's largest video-games market in 2016.[95] As an industry, video games are now worth three times as much as movies globally.[96] However, China is a daunting market for foreign firms—93 percent of total spend on Apple's iOS mobile operating system in China is spent on Chinese games, which is more localized than any other country, including Japan or South Korea.[97] No doubt, UK firms had this in mind as they participated in a 2015 Ukie (the UK video game trade association) trade mission to China.[98] Even without restrictions, UK firms would have their work cut out given local preferences, complex distribution systems, and how successful Chinese game developers and platforms have been. Still, they should have the opportunity to compete on the same terms as local developers.

China's use of censorship affects both market entry and operations in China and the cross-border provision of digital services and products. Like other digital goods and services, video games are susceptible to non-tariff, behind-the-border laws and regulations. The Great Firewall of China represents a rare case where UK digital exports face a barrier at the border. Otherwise, behind this clear market access barrier, UK firms face a complicated, opaque, and changing regulatory framework tied to content moderation that together makes for a restrictive and challenging business environment. Indicative of this, the International Intellectual Property Alliance reported that the ability of foreign firms to compete in the Chinese marketplace for all audiovisual content was even more drastically curtailed during 2019, with licensing opportunities on all distribution platforms significantly hampered, through opaque regulations, obscure content review processes, and a "soft ban" on new or never released U.S. imports.[99] Ever-changing political sensitivities in China make it even more challenging for firms to know what is and isn't allowed in their games. Nor would UK video game firms want to face arbitrary bans, like the one India has enacted against several Chinese video games.[100]

As part of this China's State Administration of Press and Publication's (SAPP) administers an opaque, unpredictable, and restrictive Chinese censorship regime that affects video game's approval and distribution. In 2018, China stopped all game license reviews, which severely affected domestic and foreign firms and game distributors (due to a restructuring of departments and new rules for video game oversight).[101] While the

actual content being censored is often not political (such as intimacy, pornography, and violence), the criteria is often vague and unevenly enforced. For example, "anything that harms public ethics or China's culture and traditions" and "anything that violates China's constitution" are both prohibited in Chinese videogames. This provides Chinese government agencies with vague and broad means to restrict games with few, if any, limits. Once SAPP started reviewing game licenses again after a nine-month hiatus, it quickly approved nearly 1,000 games, but only 30 foreign games.[102]

United Kingdom digital trade policy needs to proactively prohibit these types of barriers, even if they're not evident in their initial round of trade negotiations. This includes new rules to embed regulatory best practices so that content review processes have a clear criterion, transparent review process, and predictable timeline for review. Any licensing, permit, registration, or notification procedures related to video games should also be freely available, transparent, and non-discriminatory. This would be similar to new provisions in the USMCA trade agreement on the regulation of value-added services (like Netflix, Skype, and others), as countries have used regulations to target and discriminate against these new Internet-based services. It would also be consistent with common commitments about regulatory best practices in trade agreements. Together, these commitments would provide a clearer, more predictable market for UK video game firms and products.

MANAGING DIFFERENT DATA REALMS: LIMITING EU RESTRICTIONS, BUILDING DIGITAL FREE TRADE, AND CONFRONTING CHINA-LED DIGITAL PROTECTIONISM

The United Kingdom faces a major challenge in carving out its own approach to data-driven innovation and digital trade while managing the different, and often conflicting, data realms in the European Union and China.

Along a sliding scale of cost and restrictiveness, there's the United States' and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules (CBPR) risk-based approach to data governance and digital trade, the European Union's onerous and restrictive precautionary principle-based General Data Protection Regulation (GDPR), and finally, China's sovereignty-based model of digital control and protectionism.[103] The United Kingdom should work toward adapting to and joining the first, while managing and limiting the impact of the second, and directly countering and confronting the last. This will be challenging for UK policymakers wanting to develop a genuinely vibrant, data-driven economy and digital trade agenda.

The United Kingdom's ability to define its own digital trade agenda will be largely defined by whether the European Commission does (or does not) grant it an "adequacy" decision to allow EU personal data to be transferred to the United Kingdom. Without an adequacy determination, the United Kingdom would be deemed a "third country" for data transfers under GDPR, which would limit the ways in which EU personal data could move to the UK (such as via binding corporate rules, standard contractual clauses (SCCs), and explicit consent from the data subject).

Given its prior EU membership, the United Kingdom seems well placed to be deemed "adequate," but given the European Union's opaque and unclear assessment process and ever-changing criteria, this is far from guaranteed.[104] Slides from an EC presentation in January 2020 show it is positively disposed to granting an

adequacy determination.[105] However, it is by no means assured, given potential concerns about the UK's Investigatory Powers Act 2016 and the fact that the UK has stated it will not incorporate the Charter of Fundamental Rights of the EU (Articles 7 and 8 of this Charter constitute fundamental privacy rights and data protection rights).[106] Furthermore, the European Data Protection Board has preemptively cited a potential UK-US CLOUD Act agreement to facilitate the exchange of law enforcement data as an issue that could prohibit any onward transfer of EU personal data to the United States.[107]

Given its trade and economic engagement with the European Union, adequacy is obviously important for the United Kingdom post-Brexit. But beyond adequacy, the United Kingdom should avoid following the EU's restrictive and misguided approach to governing data privacy, digital trade, AI, and other emerging digital technologies. ITIF and the Center for Data Innovation's research shows that GDPR hurts AI development, fails to increase trust, and increases compliance costs and risks.[108]

The United Kingdom should also avoid the European Union approach to data privacy and digital trade for international reasons (as well as domestic ones). There are two key reasons why the GDPR poses a broader risk to the open, rules-based, and innovative global digital economy that the United Kingdom should want to help build.

First, the European Union does not pursue meaningful digital trade rules within the text of trade agreements. Its model text for trade negotiations highlights the role and value of digital free trade and prohibits barriers to it, but subsequent provisions outlining exceptions to these rules render them worthless as they allow a country to enact barriers if it's done in the name of privacy. It reads: "Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards."[109] Giving countries the unrestrained ability to enact whatever they want in the name of privacy is bound to be misused for protectionism. If this becomes the global norm, the global digital economy will be further fragmented.

Second, the European Union's reliance on "adequacy" determinations represents a misguided, untenable, and unrealistic approach to manage data privacy concerns around the world.[110] Its pursuit of a harmonized approach to data privacy around the world is misguided and unrealistic as only a small number of countries meet the restrictive and ever-changing criteria to be deemed adequate, and unfairly forces other countries to adhere to its interpretations of adequate privacy measures. The EC has granted adequacy to a range of mainly small countries which are former colonies, yet leaves off many major, developed countries, such as Australia, Singapore, South Korea, the United States, and others. As of September 2020, the EC has granted adequacy to Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay.[111] It only grants partial adequacy to commercial organizations in Canada. This list has barely changed in recent years, with only the addition of Japan.

On the assumption that the EU deems the United Kingdom as adequate, it then becomes an issue of whether it can develop mechanisms that limit the geographic impact this entails by pursuing agreements that allow UK firms to transfer EU personal data to other countries—the so-called onward transfer. For example, the EU-Japan adequacy determination does not allow firms to onward transfer EU personal data (absent the use of some other legal tools, such as SCCs or binding corporate rules (BCRs)).

Onward transfer agreements would alleviate—to some degree—the EU's misguided focus on geography as it relates to global data privacy governance. TechUK's paper "No Interruptions: Options for the Future UK-EU Data-sharing Relationship" proposes a hub-and-spoke model for the governance of EU personal data in the United Kingdom. It suggests the UK negotiate an agreement with the United States that is substantially similar to the EU-U.S. Privacy Shield Framework to satisfy EU concerns over the onward transfer of EU personal data from the UK to the United States.[112] The model TechUK paper refers to the Swiss-US Privacy Shield (which came into effect seven months after the EU-US Privacy Shield) as a model. However, its legal validity is in question after the Court of Justice of the European Union's (ECJ) recent decision to invalidate the EU-US Privacy Shield framework.[113] So there's no certainty that the EU would agree to such agreements between third-countries to manage EU personal data. The central focus on managing EU personal data is a clear example of how EU policy will influence post-Brexit UK digital trade policy.

Beyond the challenge of managing EU personal data, the broader United Kingdom digital trade strategy should be based on building interoperability in data governance (as mentioned earlier). Interoperability is a preferable and realistic goal for the United Kingdom (as compared to the EU's drive for a harmonized approach to data privacy) as it is based on the recognition that due to legal, social, cultural, and other factors, each country will design and enforce data privacy in different ways, but that these can be based on internationally agreed principles, such as those at the OECD. Rather than tell firms where they can store or process data, countries should hold firms accountable for managing data they collect, regardless of where they store or process it.

As per ITIF's report "Principles and Policies for "Data Free Flow With Trust," the accountability principle within this interoperability framework is based on the fact that a firm with "legal nexus" in a country's jurisdiction has to abide by its data-related laws (even if the company transfers data abroad). Focusing on this key legal nexus concept would cover the behavior of many firms that attract regulatory scrutiny. Just as a global bank or manufacturer with branches or plants in a given nation is subject to that nation's privacy and security laws and regulations, foreign technology (or any other) firms cannot escape from complying with that nation's laws by transferring data overseas.

While it doesn't get the attention that the EU's GDPR gets, this accountability- and interoperability-based approach to data governance is shared by many nations and firms, including for data privacy. For example, the majority of companies in the United States must disclose certain data-privacy practices and adhere to those requirements, even when processing data outside the country, as they remain responsible for the data regardless of where it is processed. U.S. companies mitigate these risks by stipulating requirements in relevant data-handling and processing contracts they implement with other companies. For example, foreign companies operating in the United States must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data—even if they move data outside the United States. And, if a foreign company's affiliates overseas violate HIPAA, then U.S. regulators can bring legal action against the foreign company's operations in the United States.

The accountability principle is also embedded within many data-transfer mechanisms that countries and firms use, such as model contracts, BCRs, the EU-U.S. Privacy Shield, and the APEC CBPR.[114] But given the rise of the EU and China models, countries that support the free flow of data and digital free trade need to do a much better job of explicitly calling for it and of enacting provisions that embed it in their trade agreements in order to make it the preferred global standard. It's implicitly built into the trade rules within the Comprehensive and Progressive Agreement for Trans-Pacific Partnership's e-commerce chapter, the Pacific Alliance's digital trade provisions, and the various digital economy partnership agreements involving Australia, Chile, New Zealand, and Singapore.[115] The United States has started explicitly calling for this in its trade agreements. USMCA explicitly references APEC CBPR and calls for greater cooperation to further build the global interoperability of privacy regimes.[116] So does the U.S.-Japan Digital Trade Agreement.[117]

The United Kingdom should do the same in its future trade agreements. Thus far, this realm is largely defined by countries in the Asia-Pacific and Latin America. The United Kingdom should join and support their efforts. In doing so, it'd help differentiate itself from the EU approach, in which it is currently anchored. Together, the United Kingdom and these other countries could together better advocate for their interoperability-based model.

Beyond the Text: Help UK Firms Manage Different Data Realms

While the challenge of managing differentiated data realms is not new, nor unique to the United Kingdom, Brexit does bring it into stark contrast as it's transitioning from a situation where firms didn't have to do anything different to be compliant with GDPR. But now the United Kingdom is outside the EU and has different data governance and digital trade interests. The UK government needs to help its firms navigate the transition in dealing with the costly and difficult task of complying with different country/region data-related requirements.

Survey results from Japanese firms dealing with GDPR and China's new Cybersecurity Law (CSL) are indicative of the challenge UK firms face. The report "Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms" provided new and valuable firm-level insights into the impact of GDPR and China's CSL on Japanese firms.[118] Regarding CSL, it also covers firms affected by similar restrictions in other countries, such as Vietnam, India, and Russia. The survey (conducted from April to August 2019) covers 4,000 medium- and large-sized firms, which is far larger than other surveys that studied the impact of data-related restrictions on foreign firms.

The survey's first major finding is that 5 percent of firms (around 200) said their cross-border data transfers are impacted by GDPR, while 8 percent of firms (around 320) reported the same with CSL. This headline finding on the impact is relatively large given the firms affected are likely to be the most global, innovative, and digital-intensive (which is what the authors think as well). If the impact of these data-governance laws affects the largest and most globally competitive firms in an economy, then the broader implications for economic productivity and innovation could be considerable. Additionally, the authors argue that, because approximately 20 percent of respondents said they were uninformed about the regulations, the impact may be even greater as these firms may be unaware of the relevant laws and the adverse effects these regulations will

have on their business (for example, China's CSL is still relatively new in that implementing regulations continue to be drafted, enacted, and enforced).

Another interesting finding is that GDPR acts as a de facto data localization measure in that 30 percent of firms surveyed moved the location of their data storage to inside the EU. This was despite an EU-Japan adequacy agreement to cover EU personal data. However, this is not completely surprising, as the large financial penalties and considerable uncertainty about how GDPR will be enforced compels firms to be overly cautious in how they manage data. More broadly, it highlights that such uncertainty will likely lead to costs beyond the direct financial costs associated with compliance.

For China's CSL and other countries with similar restrictions (India, Indonesia, and Russia), the impact on affected firms is considerable. The percentage of firms changing, shrinking, or even stopping their business in China is nearly 5 percent, which is far higher than what's been observed so far in the case of GDPR. Meanwhile, around 28 percent of firms have shifted data storage and processes as a result of these regulations, while another 8.7 percent have outsourced such services to local providers—something the Chinese government presumably had in mind when drafting the CSL.[119]

A major part of the challenge for UK firms is that, like many other non-EU firms engaging with GDPR, is that it represents the strictest approach they'll deal with, so they often build to that standard and use it for data from non-EU countries. While understandable from a legal compliance perspective, it also detracts from the broader benefits firms could reap from using personal data from other markets for trade and innovation that isn't allowed in the EU. This means that if the United Kingdom wants to pursue an ambitious digital agenda it'll essentially need to split it in two: between EU and non-EU data realms. Put another way, its freedom of movement to do something new and different will be restricted to whatever proportion of non-EU data its firms collect and setup systems to treat separately. It's therefore in the United Kingdom's interest to examine what domestic support it needs to provide to help its firms establish differential systems for data governance, especially if it is considering broader use of international standards, certifications, and interoperability-based frameworks and mechanisms (such as APEC CBPR) to manage global data governance.

As part of this approach, the UK would need to help its firms to manage personal data from different realms to maximize its ability to engage in broader digital trade and data-driven innovation with the rest of the world. This would involve policy guidance, legal expertise, and financial support from UK government agencies and cooperation with industry associations and individual firms.

UK firms would essentially need to develop the technical tools and policies to "ring-fence" EU personal data from personal data from other countries. There is no silver bullet (in terms of automated systems) for firms to do this. This will likely involve a suite of data mapping and tagging tools, third-party auditing and advisory services, international standards and certification mechanisms, and specialist cloud-based services. It'll also likely require government support to help firms understand, adopt, and use all these tools.

Data mapping is a system of cataloguing what data a firm collects, shows how it's used, where it's stored, and how it travels throughout the organization and beyond.[120] Specialist data compliance and consultancy firms state that initial data mapping is the biggest issue in their work with clients as they don't have the tools or

know-how to identify and capture all the data that requires specific legal, technical, and administrative management. But it's a critical step to legal compliance. For example, data mapping facilitates GDPR's mandatory requirement to maintain a written record of data processing activities, to show the basis for processing personal or sensitive data, to help perform data protection impact assessment, to manage data subject access requests, and to enable regulatory authorities the ability to understand the extent of third-party access to organizational data.[121]

However, data mapping and tagging can be technically, administratively, and legally complicated. For example, personal data can apply to several types of data, which make it possible to identify (whether directly or indirectly) a person. Firms also need to identify every database, which is not always straightforward. Software developers could be using copies of a database in development sandboxes (a testing environment for new computer code). Different business units may have their own databases. The firm, and units therein, could have backups, including on legacy systems or on their own cloud services.[122]

On top of cloud storage costs, firms may pay for third-party services to ensure data privacy compliance (as basic cloud service providers do not have visibility into the types of data customers use in the cloud). These services may also provide data mapping tools to provide visibility of data, data movement, and cloud-based content control applications (thus allowing the firm to assert control over data). These services may allow firms to respond to requests from data subjects for data retrieval and the 'right to be forgotten.'

Data mapping and management tools are often part of the suite of services and advice that specialist legal compliance, consultancy, and auditing services provide to firms to ensure they're in legal compliance. Firms increasingly use these outside advisors to provide advice, audits, and certifications to validate what they're doing complies with local laws. Many firms also use third-party audits and certifications to adopt international standards (such as from ISO) and to join APEC CBPR. For non-U.S. and EU markets, firms tend to rely on ISO standards for data controllers and processes, such as ISO 27701.[123] In particular, large firms use these auditing and advisory services as they have the resources to do expensive and complicated company-wide assessments and changes to how they manage data. They're also the ones most likely to be asked by their clients (if they're data-related intermediaries, like cloud storage providers) about how they can prove they manage their data in compliance with specific jurisdictions.

But this can be costly, time consuming, and difficult, especially for SMEs. This is why there are only dozens of companies certified under APEC CBPR, as compared to the thousands of firms registered under the former EU-U.S. Privacy Shield (which only costs a few hundred dollars for most firms, as it allows firms to self-certify that they're in compliance).[124] The APEC CBPR certification cost varies by firm and country, but it can easily cost thousands, if not tens of thousands of dollars. It can also take a few months to complete. This is why Singapore has waived or lowered fees for firms wanting to be certified, especially SMEs. It states that a third-party assessment costs between $730 and $5,900.[125] There are advantages in paying and going through APEC CBPR certification as it can also lower the cost and time involved in obtaining BCR certification in the EU and otherwise being in alignment with local privacy laws (given the overlap between the various legal requirements). One firm said that its APEC CBPR certification lowered the cost of getting the BCR by 90 percent.[126]

There is little-to-no material publicly available on how these data compliance issues impact how firms use audits, technical tools, and certifications to take advantage of new trade rules to engage in digital trade.[127] It highlights the need for further research and shows how the United Kingdom needs to consider playing a direct role (including financially) to encourage the adoption of particular tools, standards, and certification mechanisms in the future if it wants its firms to maximize the use of new commitments it pursues in trade agreements. It should also work with Australia, Japan, New Zealand, and the United States on this issue given their firms are facing the same challenge and similarly want to develop the tools and mechanisms to support digital free trade as part of a interoperability-based model.

ENDNOTES

1. "Modern Spice Routes: The Cultural Impact and Economic Opportunity of Cross-Border Shopping," Pay Pal Report, 2014, https://www.paypalobjects.com/webstatic/mktg/2014design/paypalcorporate/PayPal_ModernSpiceRoutes_Report_Final.pdf.

2. Ibid.

3. Nigel Cory, "Post-Hearing Written Submission: Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions" (The Information Technology and Innovation Foundation, April 21, 2017), http://www2.itif.org/2017-usitc-global-digital-trade.pdf; Nigel Cory, "Comments to the U.S. International Trade Commission Regarding the Digital Economy and Trade in Sub-Saharan Africa" (The Information Technology and Innovation Foundation, August 19, 2019, https://itif.org/publications/2019/08/19/comments-us-international-trade-commission-regarding-digital-economy-and); Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (The Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost; Nigel Cory, "Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers" (The Information Technology and Innovation Foundation, January 27, 2020), https://itif.org/publications/2020/01/27/surveying-damage-why-we-must-accurately-measure-cross-border-data-flows-and; Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (Information Technology and Innovation Foundation, February 24, 2015),https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries; Nigel Cory, "Submission to New Zealand's Ministry of Foreign Affairs and Trade on Objectives for Digital Economy Partnership Agreement Negotiations" (Information Technology and Innovation Foundation, July 2, 2019), https://itif.org/publications/2019/07/02/submission-new-zealands-ministry-foreign-affairs-and-trade-objectives; Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for "Data Free Flow With Trust"" (The Information Technology and Innovation Foundation, May 27, 2019), https://itif.org/publications/2019/05/27/leading-think-tank-urges-g20-adopt-core-principles-enable-free-flow-data

4. Cory, Atkinson, and Castro, "Principles and Policies for "Data Free Flow With Trust.""

5. Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"; Nigel Cory, "Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade" (The Information Technology and Innovation Foundation, June 30, 2020), https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff; Nigel Cory, "Response to the Public Consultation for the European Commission's White Paper on a European Approach to Artificial Intelligence" (The Information Technology and Innovation Foundation, June 12, 2020), https://itif.org/publications/2020/06/12/response-public-consultation-european-commissions-white-paper-european.

6. Eline Chivot and Nigel Cory, "Response to European Commission Consultation on Transfers of Personal Data to Third Countries and Cooperation Between Data Protection Authorities" (The Information Technology and Innovation Foundation, April 29, 2020), https://itif.org/publications/2020/04/29/response-european-

commission-consultation-transfers-personal-data-third; Cory, "Response to the Public Consultation for the European Commission's White Paper on a European Approach to Artificial Intelligence."

7. For example, "Australia-Singapore Digital Economy Agreement: summary of key outcomes," Australia's Department of Foreign Affairs and Trade, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-summary-key-outcomes

8. "Australia-Singapore Digital Trade Standards," TRPC presentation, March, 2020, https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-trade-standards-presentation.pdf.

9. Ravi Menon, "Singapore FinTech: Innovation, Inclusion, Inspiration: speech," November 12, 2018, https://www.mas.gov.sg/news/speeches/2018/singapore-fintech.

10. "USMCA Chapter 28: Good Regulatory Practices," USTR website, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/28_Good_Regulatory_Practices.pdf.

11. "USMCA Chapter 19: Digital Trade," USTR website, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf; "USMCA Chapter 18: Telecommunications," https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/18-Telecommunications.pdf.

12. In 2018, MAS and the U.S. Commodity Futures Trading Commission (CFTC) signed a similar MOU: https://www.cftc.gov/sites/default/files/2018-09/cftc-mas-cooparrgt091318_16.pdf; U.S. Department of the Treasury Under Secretary McIntosh stated: "Data connectivity facilitates financial regulators' access to the financial risk-related data needed to fulfil their mandates in ensuring safety and soundness….When data connectivity is impeded, firms, consumers, regulators, and the economy as a whole are all worse off, and we risk losing out on many benefits of today's digital economy, https://home.treasury.gov/news/press-releases/sm900.

13. "The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.," UK's Information Commissioner's Office, July 9, 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

14. "ICO's blog on its international work," UK's Information Commissioner's Office, https://ico.org.uk/about-the-ico/news-and-events/icos-blog-on-its-international-work/; "FTC Signs Memorandum of Understanding with UK Privacy Enforcement Agency," U.S. Federal Trade Commission website, March 6, 2014, https://www.ftc.gov/news-events/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency; "MOU Between the Privacy Commissioner of Canada and the Information Commissioner of the United Kingdom," https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-memorandums-of-understanding/mou-uk/.

15. Joshua New, "AI Needs Better Data, Not Just More Data," Center for Data Innovation blog, March 20, 2019, https://www.datainnovation.org/2019/03/ai-needs-better-data-not-just-more-data/.

16. "Data Scientist: 2017 Report" (CrowdFlower, industry report, 2017), https://visit.figure-eight.com/rs/416-ZBE-142/images/CrowdFlower_DataScienceReport.pdf.

17. Open Data Handbook, "What is Open Data?", Open Knowledge Foundation, 2012, http://opendatahandbook.org/en/what-is-open-data/.

18. Dave Nyczepir, "As data-sharing becomes more crucial, agencies say industry can help with privacy issues," *Fed Scoop,* July 8, 2020, https://www.fedscoop.com/data-privacy-government-cots-census-bureau/.

19. "Open Data Inventory," https://odin.opendatawatch.com

20. "National Data Strategy," https://www.gov.uk/guidance/national-data-strategy

21. Defined as "not a legal entity or institution, but rather a set of relationships underpinned by a repeatable framework, compliant with parties' obligations to share data in a fair, safe, and equitable way." Professor Wendy Hall and Jerome Pesenti, "Growing the Artificial Intelligence Industry in the UK," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf.

22. "Project Data Sphere® Cancer Research Platform Achieves Key Milestones: Data from More 100,000 Patients and Over 133 Research Studies," Press Release, December 13, 2017, https://www.businesswire.com/news/home/20171213005674/en/Project-Data-Sphere%C2%AE-Cancer-Research-Platform-Achieves; Joshua New, "The Promise of Data-Driven Drug Development" (The Center for Data Innovation, September 18, 2019), https://www.datainnovation.org/2019/09/the-promise-of-data-driven-drug-development/.

23. Daniel Castro, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (The Center for Data Innovation, November 6, 2017), https://www.datainnovation.org/2017/11/blocked-why-some-companies-restrict-data-access-to-reduce-competition-and-how-open-apis-can-help/.

24. "Response to the European Commission's Consultation on the European Strategy for Data" (The Center for Data Innovation, 2020), http://www2.datainnovation.org/2020-eu-data-strategy.pdf.

25. "Open Government Declaration," https://www.opengovpartnership.org/process/joining-ogp/open-government-declaration/.

26. "Artificial intelligence, digital technology and advanced production" (Organisation for Economic Cooperation and Development, 2020), https://www.oecd-ilibrary.org/sites/629af843-en/index.html?itemId=/content/component/629af843-en.

27. Stephen Ezell, "Why Manufacturing Digitalization Matters and How Countries Are Supporting It" (The Information Technology and Innovation Foundation, April, 2018), http://www2.itif.org/2018-manufacturing-digitalization.pdf.

28. Ibid.

29. Stephen J. Ezell, "A Policymaker's Guide to Smart Manufacturing," (Information Technology and Innovation Foundation, November 2016), 1, http://www2.itif.org/2016-policymakers-guide-smart-manufacturing.pdf.

30. Ben Sheridan, "Standards Outlook: Digital Transformation," bsi, https://content.yudu.com/web/43fqt/0A43ghs/IssueTwoMarch2019/html/index.html?page=10&origin=reader.

31. United Kingdom Department for Business, Energy, and Industrial Strategy (BEIS), "Industrial Strategy: Building a Britain Fit for The Future," (UK BEIS, November 2017), 205, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf.

32. Matthew Karnitsching, "Why Europe's Largest Economy Resists New Industrial Revolution," Politico EU, July 6, 2016, http://www.politico.eu/article/why-europes-largest-economy-resists-new-industrial-revolution-factories-of-the-future-special-report/.

33. "2017 Manufacturing Report" (Sikich, June 2017), 7, https://www.sikich.com/2017-manufacturing-report-download/.

34. "Technical Cooperation Program," https://www.dst.defence.gov.au/partnership/technical-cooperation-program.

35. George Costa, "Five Eyes Ministers commit to advance defence and security cooperation," *International Insider,* June 24, 2020, https://internationalinsider.org/five-eyes-ministers-commit-to-advance-defence-and-security-cooperation/; "10 U.S. Code § 2500 – Definitions," https://www.law.cornell.edu/uscode/text/10/2500.

36. "Fiscal Year 2017: Annual Industrial Capabilities: Report to Congress," U.S. Department of Defense, April 12, 2018, https://www.businessdefense.gov/Portals/51/Documents/Resources/2017%20AIC%20RTC%2005-17-2018%20-%20Public%20Release.pdf?ver=2018-05-17-224631-340.

37. "Globalization of Defense Materials and Manufacturing: Proceedings of a Workshop: Chapter: 3 Public Private Partnerships for Technology Collaboration," (The National Academies of Sciences, Engineering, and Medicine, 2018), https://www.nap.edu/read/25101/chapter/5#72.

38. Ibid.

39. "The United States and United Kingdom Sign Landmark Science and Technology Agreement," The White House, September 20, 2017, https://www.whitehouse.gov/articles/united-states-united-kingdom-sign-landmark-science-technology-agreement/.

40. "UK/USA: Agreement on Scientific and Technological Cooperation [TS No.25/2017]," https://www.gov.uk/government/publications/ts-no252017-ukusa-agreement-on-scientific-and-technological-cooperation.

41. "LLNL/U.K. officials ink agreement to collaborate on HPC research, ensure competitiveness," February 14, 2018, https://www.llnl.gov/news/llnluk-officials-ink-agreement-collaborate-hpc-research-ensure-competitiveness.

42. United Kingdom Department for Business, Energy, and Industrial Strategy (BEIS), "Industrial Strategy: Building a Britain Fit for The Future," (UK BEIS, November 2017), 205, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf.

43. The Engineer, "Made Smarter Review Makes Recommendations for Industrial Digitalization," October 30, 2017, https://www.theengineer.co.uk/digitalisation-digital-government/.

44. Catapult, "About Catapult," https://catapult.org.uk/about-us/about-catapult/.

45. Catapult, "HVM Centres," https://hvm.catapult.org.uk/hvm-centres/.

46. UK BEIS, "Industrial Strategy: Building a Britain Fit for The Future," 82.

47. Ezell, "Why Manufacturing Digitalization Matters and How Countries Are Supporting It."

48. Manufacturing USA, "How We Work," https://www.manufacturingusa.com/pages/how-we-work.

49. David M. Hart, Stephen J. Ezell, and Robert D. Atkinson, "Why America Needs a National Network for Manufacturing Innovation" (Information Technology and Innovation Foundation, December 11, 2012), https://itif.org/publications/2012/12/11/why-america-needs-national-network-manufacturing-innovation.

50. "The Institute," Digital Manufacturing and Design Innovation Institute, accessed October 4, 2016, http://dmdii.uilabs.org/the-institute/technology.

51. "About," The Institute for Advanced Composites Manufacturing Innovation, accessed October 30, 2016, http://iacmi.org/about-us/.

52. The White House, "FACT SHEET: President Obama Announces Winner of New Smart Manufacturing Innovation Institute and New Manufacturing Hub Competitions" news release, June 20, 2016, https://www.whitehouse.gov/the-press-office/2016/06/20/fact-sheet-president-obama-announces-winner-new-smart-manufacturing.

53. For example, "Australia-Singapore Digital Economy Agreement: summary of key outcomes," Australia's Department of Foreign Affairs and Trade, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-summary-key-outcomes

54. "UK joins COVID-19 High Performance Computing Consortium," Uk research and Innovation website, May 28, 2020, https://www.ukri.org/news/uk-joins-covid-19-high-performance-computing-consortium/.

55. United Nations Industrial Development Organization (UNIDO), *Role of Standards: A Guide for Small and Medium-Sized Enterprises* (Vienna: UNIDO, 2016), https://pnirajan.files.wordpress.com/2016/12/tcb_role_standards.pdf; "Understanding ICT Standardization: Principles and Practice," European Telecommunications Standards Institute, 2018, https://www.etsi.org/images/files/Education/Understanding_ICT_Standardization_LoResWeb_20190226.pdf.

56. For example, for additive manufacturing. "Standardization Roadmap for Additive Manufacturing," America Makes and ANSI, June, 2018, https://share.ansi.org/Shared%20Documents/Standards%20Activities/AMSC/AMSC_Roadmap_June_2018.pdf.

57. Office of the United States Trade Representative (USTR), "2018 National Trade Estimate Report on Foreign Trade Barriers" (Washington, D.C.: USTR, 2018), https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

58. Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (Information Technology and Innovation Foundation, December 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.

59. Richard P. Suttmeier, "A New Technonationalism?: China and the Development of Technical Standards," *Communications of the ACM,* Aril 2005, Vol 48, No 4, pages 35-37, https://cacm.acm.org/magazines/2005/4/6260-a-new-technonationalism/fulltext.

60. Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018," https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

61. Bjorn Conrad, Jaqueline Ives, Mirjam Meissner, Jost Wübbeke, and Max Zenglein, "Made in China 2025" (MERICS, August 12, 2016), https://merics.org/en/report/made-china-2025

62. Ezell and Atkinson, "The Middle Kingdom Galapagos Island Syndrome."

63. "Joint Statement: The strategic value of international standards for the UK as a global trading nation," bsi website, https://www.bsigroup.com/globalassets/documents/about-bsi/nsb/trade/bsi-strategic-value-of-international-standards.pdf; "How are standards made: Standards come from co-operation and agreement," bsi website, https://www.bsigroup.com/en-US/Standards/Information-about-standards/How-are-standards-made/.

64. Nigel Cory and Robert Atkinson, "Why and How to Mount a Strong, Trilateral Response to China's Innovation Mercantilism" (Information Technology and Innovation Foundation, January 13, 2020), https://itif.org/publications/2020/01/13/why-and-how-mount-strong-trilateral-response-chinas-innovation-mercantilism.

65. Key differences between how the European Union and United States deal with standards in trade agreements is explained in: Cory and Atkinson, "Why and How to Mount a Strong, Trilateral Response to China's Innovation Mercantilism."

66. "MOU between the Versailles Project on Advanced Materials and Standards (VAMAS) and the International Organization for Standardization (ISO), https://www.nims.go.jp/vamas/refarences/lndldd000000045h-att/MOU_VAMAS_ISO.pdf; "Versailles Project on Advanced Materials and Standards (VAMAS)," http://www.vamas.org/.

67. Ibid.

68. "Current active TWAs," http://www.vamas.org/twa/active.html.

69. "Ceramics Division: Materials Science and Engineering Laboratory: FY 2002 Programs and Accomplishments," U.S. National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6904.pdf.

70. "JRC and NIST explore further common areas of work in certified reference materials for nanotechnology and health-related measurement standards," European Commission website, March 27, 2014, https://ec.europa.eu/jrc/en/science-update/jrc-and-nist-explore-further-common-areas-work-certified-reference-materials-nanotechnology-and.

71. Gerard Riviere, "European and international standardisation progress in the field of engineered nanoparticles," *Inhal Toxicology*, Jul 21, 2009, Suppl 1:2-7, https://pubmed.ncbi.nlm.nih.gov/19558227/; Ajit Jillavenkatesa, "US-EU Workshop on Bridging nanoEHS Research Efforts," U.S. National Institute of Standards and Technology presentation, December 3, 2013, https://www.us-eu.org/wp-content/uploads/2013/12/Jilla-Slides.pdf.

72. MoUs can create a "tail wagging the dog" situation with the MOUs defining how work should happen rather than letting researchers, industry experts, and others to identify and define opportunities for pre-standardization cooperation.

73. "April 2019 - BSI's activities on Artificial Intelligence (AI)," bsi website, https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/news/april-2019---bsis-activities-on-artificial-intelligence-ai/

74. "US-UK Mutual Recognition Agreement," U.S. National Institute of Standards and Technology, https://www.nist.gov/standardsgov/us-uk-mutual-recognition-agreement.

75. "Addressing ethics in autonomous and intelligent systems," bsi website, July 25, 2018, https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/july/addressing-ethics-in-autonomous-and-intelligent-systems/.

76. "Executive Order on Maintaining American Leadership in Artificial Intelligence," White House, February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

77. "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools," U.S. National Institute of Standards and Technology, August 9, 2019, https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

78. "Framework for Improving Critical Infrastructure Cybersecurity," U.S. National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

79. "International Resources: Cybersecurity Framework," U.S. National Institute of Standards and Technology, https://www.nist.gov/cyberframework/international-resources

80. Amy Mahn, "Continuing to Strengthen International Connections on the Cybersecurity Framework," U.S. National Institute of Standards and Technology blog post, April 21, 2020, https://www.nist.gov/blogs/cybersecurity-insights/continuing-strengthen-international-connections-cybersecurity-framework.

81. "How does UK legislation match up to the NIST Cybersecurity Framework?," Quorum Cyber blog post, https://www.quorumcyber.com/blog/2018/11/21/how-does-uk-legislation-match-up-to-the-nist-cybersecurity-framework.

82. Alistair Nolan, *Artificial intelligence, digital technology and advanced production* (Paris: Organisation for Economic Cooperation and Development), https://www.oecd-ilibrary.org/sites/629af843-en/index.html?itemId=/content/component/629af843-en.

83. Michael McLaughlin, "The National Artificial Intelligence Initiative Act Could Strengthen U.S. AI Leadership" (Center for Data Innovation, March 21, 2020), https://www.datainnovation.org/2020/03/the-national-artificial-intelligence-initiative-act-could-strengthen-u-s-ai-leadership/.

84. "To Measure Bias in Data, NIST Initiates 'Fair Ranking' Research Effort," U.S. National Institute of Standards and Technology blog post, November 14, 2019, https://www.nist.gov/news-events/news/2019/11/measure-bias-data-nist-initiates-fair-ranking-research-effort.

85. "Draft White Paper on Combinatorial Methods for Explainability in AI and Machine Learning," U.S. National Institute of Standards and Technology, May 22, 2019, https://www.nist.gov/news-events/news/2019/05/draft-white-paper-combinatorial-methods-explainability-ai-and-machine.

86. "Exploring AI Trustworthiness: Workshop Series Kickoff Webinar," U.S. National Institute of Standards and Technology, August 6, 2020, https://www.nist.gov/news-events/events/2020/08/exploring-ai-trustworthiness-workshop-series-kickoff-webinar.

87. "Standards Glossary," https://www.standardsuniversity.org/article/standards-glossary/.

88. "ITU-T Telecommunication Standardization Advisory Group: Report 8 (TSAG-R8-E)," International Telecommunication Union, September 23-27, 2019, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiPrOD6gvHrAhUumnIEHekCAN8QFjACegQIAxAB&url=https%3A%2F%2Fwww.itu.int%2Fdms_pub%2Fitu-t%2Fmd%2F17%2Ftsag%2Fr%2FT17-TSAG-R-0008!!MSW-E.docx&usg=AOvVaw0n39VqhqBT8NXDXU_wmSKi.

89. "2018 Global Games Market Report," (New Zoo, industry report, 2018), https://newzoo.com/insights/articles/newzoos-2018-report-insights-into-the-137-9-billion-global-games-market/.

90. Martin Kimber, "The biggest British industry that no one's talking about," *The Article,* July 27, 2020, https://www.thearticle.com/the-biggest-british-industry-that-no-ones-talking-about.

91. James Batchelor, "GTA V is the most profitable entertainment product of all time," *GamesIndustry.biz,* April 9, 2018, https://www.gamesindustry.biz/articles/2018-04-09-gta-v-is-the-most-profitable-entertainment-product-of-all-time.

92. "ukie map," https://gamesmap.uk/#/map.

93. "With record-breaking revenue, the UK game industry is blowing up," *Venture Beat,* March 18, 2019, https://venturebeat.com/2019/03/18/with-record-breaking-revenue-the-u-k-game-industry-is-blowing-up/.

94. Nigel Cory, "Senate Testimony: Censorship as a Non-Tariff Barrier to Trade" (The Information Technology and Innovation Foundation, June 30, 2020), http://www2.itif.org/2020-censorship-ntb.pdf?_ga=2.173359072.295829696.1597152027-254668983.1577993982.

95. "Europe Meets China – How The Games Industry Is Evolving," Atomico, June 1, 2017, https://www.atomico.com/europe-meets-china/.

96. Ibid.

97. Ibid.

98. "China games trade mission a success," ukie website, July 30, 2015, https://ukie.org.uk/news/china-games-trade-mission-a-success; "Trading In China," ukie website, July 13, 2018, https://ukie.org.uk/news/trading-in-china.

99. "China: 2020 Special 301 Report on Copyright Protection and Enforcement," The International Intellectual Property Alliance, February 6, 2020, https://www.iipa.org/files/uploads/2020/02/2020SPEC301CHINA.pdf.

100. Josh Ye, "India bans Chinese games; Game engines in China; Cheatware market reaches 293m; IGN's China relaunch -- China Gaming News Roundup," Kaeland, September 6, 2020, https://kaleland.substack.com/p/india-bans-chinese-games-game-engines.

101. Rick Lane, "China freezes all game license approvals," *PC Gamer*, August 15, 2018, https://www.pcgamer.com/china-freezes-all -game-license-approvals/; Shannon Liao, "Apple blames revenue loss on China censoring video games," *The Verge*, January 29, 2019, https://www.theverge.com/2019/1/29/18202812/chinese-censorship-hurt-apples-bottom-line.

102. "Nearly 1,000 games have received a license since the restart of game approvals in China," Niko Partners, 2019, https://nikopartners.com/nearly-1000-games-have-received-a -license-since-the-restart-of-game-approvals-in-china/.

103. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (The Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost; Nigel Cory, "China and the United States: Digital Protectionism vs. Digital Free Trade" (The Information Technology and Innovation Foundation, October 18, 2019), https://itif.org/publications/2019/10/18/china-and-united-states-digital-protectionism-vs-digital-free-trade; Nigel Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules" (The Information Technology and Innovation Foundation, May 9, 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

104. Eline Chivot, "Not Granting GDPR Adequacy to the UK Would Be a Mistake," Center for Data Innovation blog post, September 14, 2020, https://www.datainnovation.org/2020/09/not-granting-gdpr-adequacy-to-the-uk-would-be-a-mistake/.

105. Emmanuel Ronco, Natalie Farmer, and Tom Wales, "Cleary Cybersecurity and Privacy Watch," Cleary Gottlieb website, January 22, 2020, https://www.clearycyberwatch.com/2020/01/european-commission-provides-further-hints-at-post-brexit-adequacy-decision-for-the-uk/.

106. Nicole Kobie, "The UK's data sharing deals with Europe are about to get real messy," *Wired,* February 18, 2020, https://www.wired.co.uk/article/brexit-data-protection-gdpr.

107. Alex Scroxton, "UK-US data deal puts Brexit data adequacy pact at risk," *ComputerWeekly.com,* June 16, 2020, https://www.computerweekly.com/news/252484726/UK-US-data-deal-puts-Brexit-data-adequacy-pact-at-risk.

108. Eline Chivot and Daniel Castro, "What the Evidence Shows About the Impact of the GDPR After One Year" (The Center for Data Innovation, June 17, 2019), https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/; Eline Chivot and Daniel Castro, "The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy" (The Center for Data Innovation, May 13, 2019), https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/; Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI" (The Center for Data Innovation, March 27, 2018), http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

109. Nigel Cory, "EU Digital Trade Policy Proposal Opens a Loophole for Data Protectionism," *Euractive,* July 16, 2018, https://itif.org/publications/2018/07/16/eu-digital-trade-policy-proposal-opens-loophole-data-protectionism.

110. Chivot and Cory, "Response to European Commission Consultation on Transfers of Personal Data to Third Countries and Cooperation Between Data Protection Authorities."

111. "Adequacy decisions," European Commission website, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

112. techUK, "Rapid Action Needed to Safeguard UK & EU Businesses & Consumers Following Brexit" (techUK, industry report, November 30, 2017), https://www.techuk.org/insights/news/item/11824-rapid-action-needed-to-safeguard-uk-eu-businesses-consumers-following-brexit.

113. Alaap Shah, Audrey Davis, Karen Mandelbaum, and Matthew Berger, "ECJ Invalidated the EU-US Privacy Shield Framework," *National Law Review,* July 28, 2020, https://www.natlawreview.com/article/ecj-invalidated-eu-us-privacy-shield-framework.

114. For example, firms may implement (and demonstrate) accountability through various internal privacy and information management programs, regulated frameworks (such as the EU's Binding Corporate Rules and the EU-US Privacy Shield), industry codes of conduct, third-party certifications and seals, and international standards. Binding corporate rules state firms may transfer personal data across borders within a single company. See: "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society" (Center for Information Policy Leadership, July 23, 2018), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

115. "Comprehensive and Progressive Agreement for Trans-Pacific Partnership text and resources," https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text-and-resources/; "Additional Protocol To The Framework Agreement Of The Pacific Alliance," https://www.global-regulation.com/translation/colombia/6405370/through-which-the-%2526quot%253badditional-protocol-to-

the-framework-agreement-of-the-pacific-alliance%2526quot%253b%252c-signed-in-cartagena-de-indias%252c-repub.html; "Digital Economy Partnership Agreement (DEPA)," https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/.

116. "USMCA: Chapter 19: Digital Trade," USTR website, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

117. "U.S.-Japan Digital Trade Agreement," USTR website, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

118. Eiichi Tomiura, Banri Ito, and Byeongwoo Kang, "Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms" (Research Institute of Economy, Trade and Industry, November, 2019), https://www.rieti.go.jp/jp/publications/dp/19e088.pdf.

119. Cory, "Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers."

120. "Brexit update – the shape of the United Kingdom's exit," Evershed Sutherland website, January 29, 2020, https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Brexit/shape-of-uk-exit-290120.

121. Chandra Shekhar, "Data Mapping and GDPR: How Are They Related?," Develops.com, July 2, 2019, https://devops.com/data-mapping-and-gdpr-how-are-they-related/.

122. Richard Macaskill, "So, What is Data Mapping and Why is it the Key to GDPR Compliance?," DataVersity website, April 25, 2018, https://www.dataversity.net/data-mapping-key-gdpr-compliance/#.

123. "ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," https://www.iso.org/standard/71670.html.

124. "Privacy Shield Framework FAQs – General," https://www.privacyshield.gov/article?id=General-FAQs.

125. "Fact Sheet: Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems Certification," Singapore's Infocomm Media Development Authority, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/PDP-Seminar-2019/2019-07-17-Fact-Sheet-for-CBPR-PRP-FINAL.pdf?la=en

126. "Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR System" (Information Integrity Solutions, February 2016), https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/591bbd6146c3c4823961ecb3/1494990185553/IIS+-+APEC+CBPR+Benefits+Paper+Final+Publicly+Released+Version+-+APEC+Communications+Unit.pdf.

127. This is, in part, due to the fact that some large firms see this capability not as a cost, but as a commercial opportunity—privacy compliance as a competitive differentiator.