TheCityUK

EY
Building a better working world

THE FUTURE UK-US TRADING RELATIONSHIP:

Creating a transatlantic digital market in services

September 2019

@thecityuk www.thecityuk.com

About TheCityUK

TheCityUK is the industry-led body representing UK-based financial and related professional services. In the UK, across Europe and globally, we promote policies that drive competitiveness, support job creation and ensure long-term economic growth. The industry contributes 10% of the UK's total economic output and employs 2.3 million people, with two thirds of these jobs outside London. It is the largest tax payer, the biggest exporting industry and generates a trade surplus greater than all other net exporting industries combined.

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

CONTENTS

FOREWORD

As commerce becomes increasingly digital, the rules governing digitally-enabled trade will play a central role in shaping the future of international business. Those countries that take the lead in liberalising digital trade will be in pole position to benefit from the digitalisation of the global economy.

The UK should aspire to play a prominent role in developing these new rules. Across the world, professional services constitute the most digitalised sectors within national economies, and services account for more than 80% of the UK's GDP. The UK is a leading international financial centre and its financial and related professional services businesses are already major players in global digital trade.

While the UK is therefore well-positioned to benefit from cross-border digital trade, it should also recognise the dangers posed by regulatory divergence on the rules by which digital trade is governed. It must work with key allies and trading partners to create a more integrated global digital market.

The UK-US trading relationship is a natural place for the UK to start when considering how to develop international co-operation around e-commerce. This is one of the world's largest and most successful partnerships. The US is the UK's largest single-country trade partner and UK businesses annually invest over $540bn (£409bn) in the US. This amounts to nearly 20% of all foreign direct investment into the US. Correspondingly, businesses in the US invest more than $757bn (£573bn) into the UK annually. At the same time, the transatlantic market is at the heart of both global finance and global data flows.

The foundations for creating a transatlantic digital market in services have already been laid. The UK and US governments and regulators enjoy deep and longstanding ties based on mutual trust and cooperation. As the UK prepares to leave the European Union, decision makers in the UK and US have established senior-level bodies to explore the prospects for an ambitious future trade agreement alongside a programme to increase regulatory co-operation between the two countries both before and after Brexit, bringing the two markets closer still.

Meanwhile, the UK and US financial and professional services industries are collaborating more closely than ever on a range of common interests. For example, TheCityUK co-chairs the transatlantic US-UK Financial and Related Professional Services Coalition, a leading example of this strong partnership approach.

This paper provides decision makers in the UK and US with a range of asks from the UK-based financial and professional services industry regarding the future of digital trade. It serves to frame the options available to governments, regulators and industry to facilitate better data flows between our countries.

The creation of a world-leading transatlantic digital market will boost jobs and growth in both jurisdictions, and provide consumers of financial and professional services with more choice and diversity of products. At a time when the established order of world trade faces significant challenges, the creation of a transatlantic digital market could serve as a reminder of the benefits that liberalisation can deliver for consumers everywhere, and serve as a leading light for international trade in a digital age. This is the goal that the UK-based financial and professional services industry aspires to, and to which this report seeks to contribute.

Miles Celic

Chief Executive Officer, TheCityUK

FOREWORD

The global economy is being reshaped by digital technology, and innovations in data use. In financial services, personal data is used to detect fraud, manage risk, monitor financial market activity, and develop personalised products. Technology continues to drive change at pace. Robotic process automation, artificial intelligence and machine learning all rely on – and create – ever growing data pools. But, as data driven innovations expand the horizons of Financial Services, and open up markets to new entrants, countries are creating barriers to trade – like data localisation – and regulators are learning how to use digital technology and data driven insights to support their own role.

Following an exit from the European Union, the UK will have the ability to negotiate their own trade agreements, and is looking to forge ambitious relationships with partners around the world. It will have greater scope to respond on its own terms to opportunities and risks in a changing data landscape. This ambitious report begins to answer many of the difficult questions about the realities of trade in the digital era. In it, you will read about recent developments in cross-border data flows and their impact on future trade agreements. You will read about new innovations in policy and regulation that will help to deliver open markets to the benefit of consumers in the UK, US and elsewhere. And you will read about new areas of innovation in across financial services, and how trade negotiations could be used to support growth in this crucial sector for 'UK PLC'.

In writing this report, we used as our focus the potential for deeper cross-border cooperation with the USA. But the principles we articulate are equally applicable to the UK's relationship with other trading partners. Whatever your perspective, I hope you find the content useful, and interesting.

Steve Holt

Partner, EY

EXECUTIVE SUMMARY

The importance of financial and related professional services (FRPS) to the UK economy is beyond doubt. As the industry becomes increasingly digitalised, its ability to continue to innovate and provide customers around the world with a range of products that suit their needs will become increasingly reliant on the terms by which firms can exchange data internationally. A more integrated global digital market will lead to growth, innovation and jobs; a more fragmented global digital market could hold the industry back, and deny customers the services they need.

This paper explores how the UK-based FRPS industry can work with the UK government and regulators and counterparts in the US to help create a transatlantic digital market. London and New York are the world's two leading international financial centres. If the UK-based and US-based FRPS industries can work together to create a digital transatlantic market it would result in a number of immediate benefits to both financial centres. The creation of such a market could also help shape global standards around digital trade for the industry and show stakeholders around the world what is possible when countries work together to facilitate digital trade.

This report is written from the perspective of the UK-based FRPS industry and presents a number of UK industry asks around how a transatlantic market could be created. Some of these asks could be achieved through government-to-government dialogue; others would require regulator-to-regulator dialogue; and some would need to be led by the UK and US-based industries. However, in order for the broad goal of a transatlantic digital market to be achieved it will be essential for industry, government and regulators to work together on both a national and cross-border basis.

The report is split into four short sections, each with a specific focus:

1. A framework for UK-US cooperation on digital trade – outlining a number of mechanisms that are available to the industry, government and regulators to create a transatlantic digital market.

2. Cross cutting industry asks – detailing the asks that the UK-based FRPS industry has relating to the creation of a transatlantic digital market. These relate to areas that affect the entire industry (and in many cases other sectors of the UK economy too), such as avoiding data localisation restrictions, facilitating the exchange of personal data between the UK and the US and advancing cooperation between the two countries in areas such as national security, financial crime and RegTech.

3. Sector specific examples – setting out the asks relevant to specific sectors of the industry regarding the creation of a digital transatlantic market. Sectors covered include payments, open banking, consumer credit, wealth and asset management, pensions, insurance and professional services such as legal services and accountancy.

4. Evidence base and industry asks – in writing this report we have collated information from a wide variety of secondary sources through interviews with members of TheCityUK and distilled this as much as possible into reference tables. This section contains a summary table of proposed industry asks, and a number of examples of countries that have data localisation laws in place.

1. A FRAMEWORK FOR UK-US COOPERATION ON DIGITAL TRADE

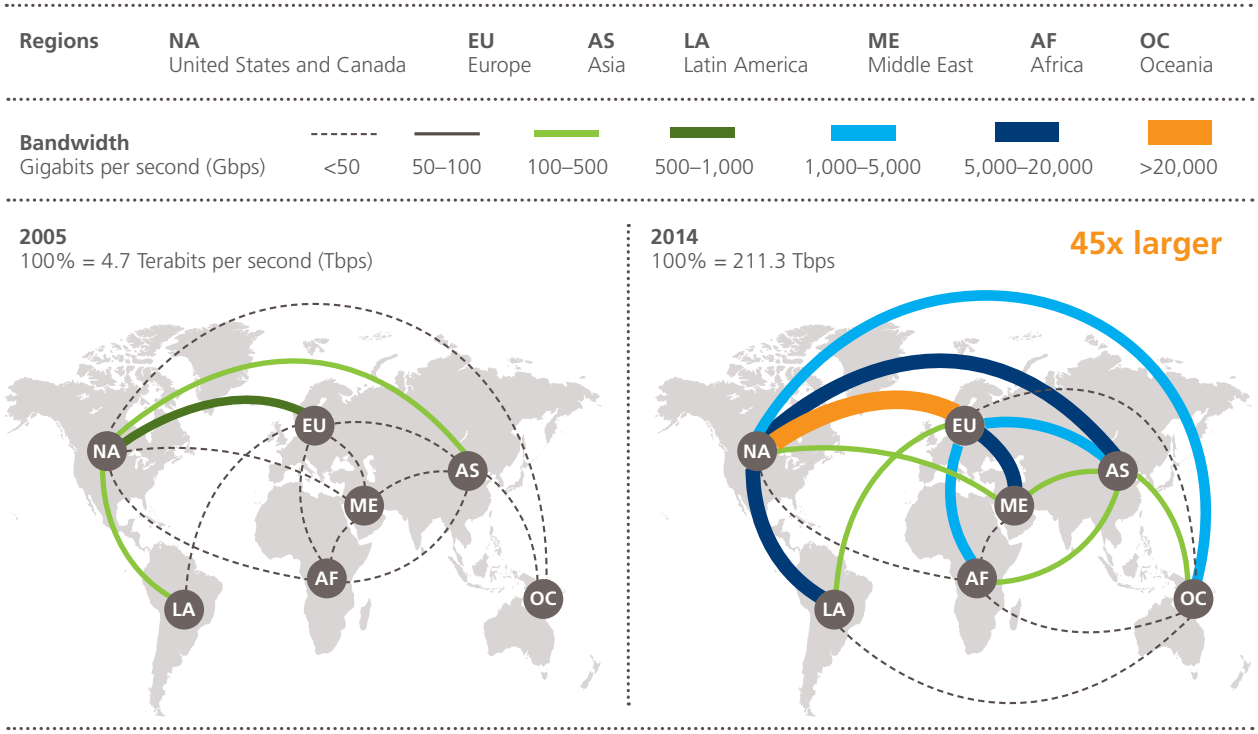
The UK and the US are the world's two most important international financial centres.[1] Both countries command deep and liquid markets, unrivalled financial infrastructure and unique expertise across the range of FRPS. Across many industry sectors, from fixed income and commodity trading to clearing services, commercial insurance, reinsurance, asset management, legal services, accounting and consulting, the UK and US make up both first and second place in global rankings.[2] The global predominance of the UK and US in global finance is underpinned by the fact that they possess the world's most sophisticated regulatory regimes and well-resourced and knowledgeable regulators. With such advanced and developed FRPS ecosystems in place, it is unsurprising that the two countries are the greatest facilitators of investment overseas and have historically played a leading role in influencing the setting of global standards for the industry.

However, the industry is changing rapidly. As new technologies develop, FRPS is becoming increasingly digitalised. The pace of digitalisation is different from sector to sector. Aspects of banking and capital markets are almost unrecognisable from 20 years ago. The speed of change in other sectors is less striking. But even in sectors such as legal services, where traditional business models have proven more enduring, new technologies are changing how practitioners work.

The UK and the US are currently at the forefront of digital innovation in FRPS. This can be seen by their pre-eminence in FinTech (and equivalent technologies such as RegTech and LawTech): New York, London and San Francisco are widely recognised as the world's leading FinTech hubs. More widely, however, the extent of data flows between the industries on both sides of the Atlantic provides ample evidence of the strength and depth of the relationship.

Figure 1: Used cross-border bandwidth

Source: TeleGeography, Global Internet Geography; McKinsey Global Institute analysis



NOTE: Lines represent interregional bandwidth (e.g. between Europe and North America) but exclude intraregional cross-border bandwidth (e.g. connecting European nations with one another).

[1] See, for example, the widely used Z/Yen index of leading international financial centres: New York is ranked first and London a very close second.
[2] TheCityUK, 'A vision for a transformed, world-leading industry', (July 2017), available at: https://www.thecityuk.com/research/a-vision-for-a-transformed-world-leading-industry/

The transatlantic market is the most active site for cross-border data flows in the world. A McKinsey survey of used cross-border bandwidth (a substitute figure for data flows) in 2014 showed that US-Europe data exchange stood at over 20,000 gigabits per second, far ahead of trade between other regions. The scale of data flows will have increased significantly since 2014, but the centrality of transatlantic data flows is a long established trend, and results in part from the fact that advanced economies are generally more connected than developing countries, and that the US and Europe are the two largest producers of digital content for internet users.[3]

Despite the strong existing digital trade links between the US and Europe, barriers still remain. Tackling those barriers, and facilitating seamless digital trade between the UK and US FRPS industries will bring tangible benefits: it will reduce the cost of engaging in international trade, facilitate the coordination of global value chains and, perhaps most importantly, will connect a greater number of businesses and customers globally.

For decades, much of the industry in the UK and the US has sought to move towards a single transatlantic marketplace, which would allow businesses to grow and customers and end-users in both markets to benefit from greater choice and competition. Creating such a market has not proven easy: regulatory divergence between the US and EU since the global financial crisis in 2008, the failure to conclude the Transatlantic Trade and Investment Partnership (TTIP) negotiations and political dynamics on both sides of the Atlantic have all hindered progress.

However, despite these difficulties, digital trade between the FRPS industries in the UK and US is growing, helping to bring the two markets closer together. There is now significant potential for businesses, governments and regulators to use new technologies and standards governing the use of these technologies to help make a single transatlantic market into a reality.

In light of their shared aim of maintaining their world-leading FRPS industries and building a single transatlantic marketplace, the US and UK have established a Financial Innovation Partnership. This partnership seeks to promote collaboration between the US Department of the Treasury and HM Treasury, through deepening bilateral approaches to emerging trends in FRPS innovation. It intends to focus on regulatory engagement – identifying and addressing potential regulatory synergies to develop a closer working relationship – and commercial engagement, though exploiting increased opportunities for the US and UK FRPS industries to share information and expertise around promoting growth and innovation.

This is a strong start in terms of collaboration, which can be facilitated even further if FRPS organisations in both markets are able to exchange data and digital products and services in a framework facing fewer restrictions. This paper suggests ways in which industry, governments and regulators in both the UK and US can continue to take advantage of new technologies and the regulations surrounding them to help create a single transatlantic market for the FRPS industry. We recognise that this is no simple task. This paper outlines options and asks covering all sectors of the industry. Some of these could be acted upon by the industry itself; others would need to be taken up by UK and US government departments (for example, the UK and US Treasuries working in concert) or would need a response by regulators. But it is clear that in order to be successful, stakeholders' efforts will need to be coordinated. On the UK side, the UK-based industry, government and regulators will need to work closely together to secure the goals outlined in this paper.

[3] McKinsey & Company, 'Digital globalization: The new era of global flows', (February 2016), available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

Mechanisms for bringing about a transatlantic market for digital trade in financial and related professional services

Achieving a deeper relationship could be achieved by a combination of:

- A bilateral trade agreement, reducing barriers to trade and investment. This would need to include provisions for the avoidance of trade and investment barriers to data movement, such as data-localisation requirements and restrictions on data transfer and data processing.
- A plurilateral or multilateral trade agreement on e-commerce (or digital trade), negotiated at World Trade Organization (WTO) level.
- Agreements on regulatory coherence, such as mutual recognition agreements to build regulatory cooperation with regards to data to help regulators on both sides anticipate and resolve regulatory problems in ways that support open FRPS markets and avoid conflicts of laws which may deny consumers the choice they need.
- An agreement on the terms on which protected personal data can be transferred between the two countries. In the case of the UK, this will need to reflect the data-protection regime that the UK operates post-Brexit. It is likely to be a free-standing agreement.

These related mechanisms all provide ways of advancing UK-US trade and cooperation on digital trade. More information about each is provided below.

UK-US bilateral trade agreement

Since the UK voted to leave the EU in June 2016, the UK government has set out its intention to prioritise an ambitious new UK-US trade agreement after Brexit. In July 2017, the Department for International Trade (DIT) established a UK-US Trade and Investment Working Group to lay the ground for a potential UK-US trade agreement, including formulating requirements on data.

Meanwhile, the US government has been equally clear that it sees great value in a UK-US trade agreement. The Office of the United States Trade Representative (USTR) has set out the priorities that it will pursue in trade negotiations with the UK. Significantly, the USTR believes that a US-UK free trade agreement (FTA) could "provide an opportunity to develop new approaches to emerging trade areas where the United States and the UK share common interests and are global leaders, such as digital trade and financial services." As with other trade partners, the USTR wants an agreement which includes "state-of-the-art commitments to ensure that the UK refrains from imposing measures in the financial services sector that restrict cross-border data flows or that require the use or installation of local computing facilities."[4]

Trade agreements often include provisions that seek to improve market access and limit data-related barriers to trade, such as restrictions on data processing or data localisation requirements. When barriers to data processing or cross-border transfers are permitted under FTAs, there is often an attempt to ensure that any measures must be justified on legitimate public policy grounds and follow a least trade restrictive approach. FTAs should aim to ensure that legitimate concerns in areas such as privacy and data protection are not misused as justifications for protectionist trade measures. However, in FTAs to date, the UK (as an EU member) and US have approached these issues quite differently.

[4] United States Trade Representative, 'United States-United Kingdom Negotiations', (February 2019), available at: https://ustr.gov/sites/default/files/Summary_of_U.S.-UK_Negotiating_Objectives.pdf

- **Data processing:** the carrying out of operations on data, especially by a computer, to retrieve, transform, or classify information.
- **Data localisation:** storing user data in a data centre on the Internet that is physically situated in the same country where the data originated.
- **A Free Trade Agreement:** a treaty between two or more countries to facilitate trade and eliminate trade barriers. FTAs are arguably the most comprehensive form of bilateral trade agreements that can be reached; they can lead to deep, long term gains for both partners in the form of increased jobs and growth. Under WTO rules, FTAs must cover 'substantially all trade' between the parties, if they are to be exempted from the WTO most-favoured nation (MFN) rule (see box on page 11). A typical FTA will include general (horizontal) provisions which apply to all goods and services and sector specific (vertical) provisions set out in chapters on areas such as financial services, agriculture and telecommunications. Barriers to digital trade tend to be covered in FTA chapters on e-commerce. However, chapters on services, investment, financial services and telecommunications may also provide additional provisions on data.

The US has led the way in advocating for openness in digital trade and has pursued increasingly ambitious trade agreements. Currently awaiting ratification, the recently agreed trilateral agreement between the US, Mexico and Canada (USMCA) is the most far-reaching FTA with respect to digital trade and offers good insights into the potential US starting point in negotiations with the UK. Provisions of USMCA relating to digital trade generally aim at either banning/prohibiting certain practices, or encouraging new behaviours.

Banning/prohibiting practices:

- Ban cross-border data flow restrictions and data localisation requirements. In previous US trade agreements, financial services were excluded from these restrictions on data localisation, but the USMCA prohibition on data localisation covers financial services.
- Prohibit customs duties on digital products.[5]
- Prohibit requirements for source code disclosure or transfer as a condition for market access and further prohibits governments from requiring the disclosure of algorithms expressed in that source code except in certain clearly defined and restricted circumstances.
- Prohibit requiring technology transfer or access to proprietary information for products using cryptography.

Encouraging new behaviours:

- Require parties to have online consumer protection and anti-spam laws and a legal framework on privacy.
- Clarify intellectual property right (IPR) enforcement rules to provide criminal penalties for trade secret cyber theft.
- Promote cooperation on cybersecurity.
- Safeguard cross-border electronic card payment services.
- Cover mobile service providers and promote cooperation for international roaming charges.
- Allow internet platforms to benefit from a 'safe harbour' which provides some protection from domestic regulation by the parties based on content they display.
- Make internet platform providers no longer liable for the actions of their users (although this provision under civil law has been subject to bipartisan challenge in the US House of Representatives).[6]

[5] European Centre for International Political Economy, 'The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions', (August 2019), available at: https://ecipe.org/publications/moratorium/

[6] Congress of the United States, 'Committee on energy and commerce', (August 2019), available at: https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/USTradeRep.2019.8.6.%20Letter%20re%20Section%20230%20in%20Trade%20Agreements.pdf

The UK, on the other hand, has until now participated in the EU's FTA negotiations with third countries and is a party to several EU agreements on facilitating trade in services. However, even where these FTAs contain financial services chapters, they do not entirely liberalise data-movement in relation to the sector and contain exceptions. The EU-Canada Comprehensive Economic and Trade Agreement (CETA), signed in 2016 and in provisional operation, is a good example of this. Its trade in services chapter excludes financial services (Article 9.2), and its financial services chapter contains exceptions allowing the parties to restrict the movement of "any confidential information which, if disclosed, would interfere with specific regulatory, supervisory, or law enforcement matters, or would otherwise be contrary to public interest or prejudice legitimate commercial interests of particular enterprises" (Article 13.17(2)).

- **Most-favoured-nation:**
  Under the WTO agreements, countries cannot normally discriminate between their trading partners. If a WTO member accords favourable treatment (such as a reduced rate of duty on an import), the most-favoured-nation (MFN) rule requires it to do so for all other WTO members (unless the treatment was accorded in the context of a deeper bilateral or plurilateral trade agreement qualifying for exemption from the MFN rule).
- **National treatment:**
  Imported and locally-produced goods and services should be treated equally once foreign products have entered the market. The same should apply to foreign and local trademarks, copyrights and patents.

Agreement on e-commerce at the WTO

In recent years, the impetus for cooperation on digital trade issues has principally been at a bilateral level. However, a large number of WTO members have recently begun work in the WTO framework towards an agreement on e-commerce (current WTO terminology for digital trade).

The WTO Agreements (resulting in 1994 from the General Agreement on Tariffs and Trade (GATT) Uruguay Round of trade negotiations) predated the development and widespread use of the internet. Nonetheless, they provide much of the basis of international cooperation on digital trade and set the template for many of the bilateral agreements that followed. Although the General Agreement on Trade in Services (GATS) 1994 did not specifically contemplate digital trade as it now exists, its basic principles of non-discrimination, such as the most-favoured nation (MFN) rule and the importance of national treatment (NT), are applicable to digital trade.

In January 2019 a number of WTO members, including the US and the EU, confirmed their intention to begin WTO negotiations on trade-related aspects of electronic commerce with a view to achieving a high standard outcome building on existing WTO agreements and frameworks with the participation of as many WTO Members as possible. This Joint Statement Initiative (called after the Joint Statement at the WTO Eleventh Ministerial Conference (MC11), Buenos Aires, December 2017) was backed by a further statement by Trade Ministers meeting at Davos in the margins of the World Economic Forum in January 2019. Participants in the G20 Osaka Summit (28-29 June 2019) endorsed the Joint Statement Initiative and reaffirmed the importance of the WTO Work Programme on electronic commerce. At the time of writing, negotiations in the WTO framework are continuing.

Excerpt from G20 Osaka leaders' declaration, July 2019

Innovation: digitalisation, data free flow with trust

Innovation is an important driver for economic growth, which can also contribute to advancing towards the SDGs and enhancing inclusiveness. We will work toward achieving an inclusive, sustainable, safe, trustworthy and innovative society through digitisation and promoting the application of emerging technologies. We share the notion of a human-centred future society, which is being promoted by Japan as Society 5.0. As digitalisation is transforming every aspect of our economies and societies, we recognise the critical role played by effective use of data, as an enabler of economic growth, development and social well-being. We aim to promote international policy discussions to harness the full potential of data.

Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow with trust will harness the opportunities of the digital economy. We will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development. We also reaffirm the importance of interface between trade and digital economy, and note the ongoing discussion under the 'Joint Statement Initiative' on electronic commerce, and reaffirm the importance of the Work Programme on electronic commerce at the WTO.

To further promote innovation in the digital economy, we support the sharing of good practices on effective policy and regulatory approaches and frameworks that are innovative as well as agile, flexible, and adapted to the digital era, including through the use of regulatory sandboxes. The responsible development and use of Artificial Intelligence (AI) can be a driving force to help advance the SDGs and to realise a sustainable and inclusive society. To foster public trust and confidence in AI technologies and fully realise their potential, we commit to a human-centred approach to AI, and welcome the non-binding G20 AI Principles, drawn from the 'Organisation for Economic Cooperation and Development' (OECD) Recommendation on AI. Further, we recognise the growing importance of promoting security in the digital economy and of addressing security gaps and vulnerabilities. We affirm the importance of protection of intellectual property. Along with the rapid expansion of emerging technologies including the Internet of Things (IoT), the value of an ongoing discussion on security in the digital economy is growing. We, as G20 members, affirm the need to further work on these urgent challenges. We reaffirm the importance of bridging the digital divide and fostering the adoption of digitalisation among micro, small and medium enterprises and all individuals, particularly vulnerable groups and also encourage networking and experience-sharing among cities for the development of smart cities.

The UK is currently involved in the WTO negotiations as a member of the EU and will continue to be involved independently after Brexit. It will be important for the UK to pursue progress on digital trade in the WTO framework, in a way that takes account of UK FRPS interests, including those covered in this report. It will also be important for UK negotiators in UK-US trade talks to have regard to progress in the WTO negotiations when considering the scope and substance of any UK-US agreement. It may be that breakthroughs on certain issues can be made more easily as part of multilateral discussions than bilateral discussions.

Regulatory cooperation

Financial regulators in the UK and the US have long worked together to tackle common challenges and have developed strong ties of trust and confidence in the process. This partnership has, if anything, deepened in the aftermath of the UK's decision to leave the EU, when the UK and US Treasuries established a US-UK Financial Regulatory Working Group to explore how to develop further cooperation around financial regulation. HM Treasury has recently published a joint statement by members of this Group, following discussions on the outlook for financial regulatory reforms and future priorities, including possible areas for deeper regulatory cooperation. They also discussed the impact of the UK's exit from the EU on financial stability and cross-border financial regulation.[7]

Both the UK and US FRPS industries have strongly supported further cooperation and set up an industry-led, joint US-UK FRPS Coalition to advise both governments on how to proceed with regulatory cooperation and provide industry input into these intergovernmental Treasury-to-Treasury meetings.

The industry supports UK-US regulatory cooperation because it can improve market access, facilitate more effective tax and enforcement initiatives and strengthen national security, especially in relation to financial crime and cyber security. Moreover, an ambitious agreement on regulatory cooperation would position both countries strongly in the future setting of global standards and improve efficiency in FRPS worldwide.

The UK and the US have traditionally taken distinct approaches to regulation. Since its accession to the European Communities in 1973, the UK has become subject to a growing range of EU regulation, which is frequently based on a highly centralised and precautionary model. US regulation tends to be more risk-based (otherwise known as science-based) and in many sectors of the industry the US pursues a decentralised approach to regulation.[8] Given the dangers of regulatory divergence, UK-US trade negotiators should focus on setting realistic goals for a framework for continued regulatory collaboration. Equally, in the pursuit of a collaborative framework, the UK and US must consider the risks of limiting their ability to set and maintain their own domestic prudential rules.

An increase in UK-US regulatory cooperation is likely to deliver economic benefits, but any agreement will need to be carefully constructed so that regulatory cooperation respects each party's sensitivities over national autonomy. Regulators are understandably concerned to protect their independence: in the TTIP negotiations, US regulators effectively rebuffed EU proposals to include binding provisions on regulatory cooperation in financial services.[9] Regulators are often particularly wary of subjecting any regulatory feature in a trade agreement to dispute settlement procedures. It is possible, therefore, that successful regulatory cooperation between the UK and US in the future is more likely to be based around models such as mutual regulatory recognition, which preserves autonomy, rather than harmonisation or an outcomes-based approach, which may not.

- **Mutual Recognition:** an international agreement by which two or more countries agree to recognise one another's conformity assessments. In the EU, the principle of mutual recognition stems from Regulation (EC) No 764/2008. It defines the rights and obligations for public authorities and enterprises that wish to market their products in another EU country. The regulation also defines how a country can deny mutual recognition of a product.

[7] HM Treasury, 'US-UK Financial Regulatory Working Group Joint Statement', (May 2019), available at: https://www.gov.uk/government/news/us-uk-financial-regulatory-working-group-joint-statement

[8] House of Commons International Trade Committee, 'UK-US Trade Relations', (April 2018), available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmintrade/481/481.pdf

[9] European Commission 'Upgrading EU financial regulatory cooperation with the United States', (July 2016), available at: https://ec.europa.eu/newsroom/fisma/item-detail.cfm?item_id=33100

Regulatory barriers to creating a single transatlantic market in data

While current arrangements for UK-US services trade generally work well and FRPS firms enjoy a relatively good level of market access, particularly when the US is compared to other non-EU countries, regulatory barriers still exist for the FRPS industry. Obstacles to seeking greater regulatory coherence on data include:

- The US and UK regulatory regimes are built around different frameworks: in the UK, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) are largely responsible for supervising the financial services industry, whereas the model in the US is to have one regulator for each sub-sector of financial services.
- Unlike the UK, the US does not have a regulatory body with the powers to oversee and enforce data protection laws at a federal level.

The fact that much of US FRPS regulation is at a sub-federal level presents further barriers to creating a digital transatlantic market. However, examples such as the US National Association of Insurance Commissioners model laws show that such barriers can be overcome. Both governments would need to explore options for addressing such features, learning from other examples, such as insurance. One way of creating a clear mechanism for regulatory cooperation is to develop some ground rules for how regulators can work together; should this model be adopted, it would be possible to include sub-federal bodies, including state regulators and judiciaries, in negotiations. There is a precedent for this approach in the EU-Canada CETA negotiations, in which the Canadian Provinces were engaged from an early stage. When it comes to regulatory cooperation, regulators in the UK should invest time in developing links with US state regulators, initially prioritising the states with the largest FRPS markets in the US.

Although a framework for regulatory cooperation can be included within the architecture of an FTA, it is equally possible for regulatory arrangements to be placed outside an FTA allowing regulators to work together to remove restrictions and develop common standards. Either way, it would remain critical for regulators on both sides of the Atlantic to continue to build on their existing strong relationships, and to work through bodies like the US-UK Financial Regulatory Working Group and engage with industry collectives such as the US-UK FRPS Industry Coalition.

Agreement on sharing personal data between the two countries

Personal data is generally subject to higher levels of protection than most other forms of data. Under current UK legislation, which incorporates the EU's General Data Protection Regime (GDPR), the personal data of EU (and currently UK) citizens cannot be freely exchanged with and processed by US-based businesses. Businesses who wish to share personal data in the transatlantic market need to make use of mechanisms such as Binding Corporate Rules (BCRs) or Standard Contractual Clauses (SCCs). The EU and the US have developed a more formal mechanism under which the personal data of EU citizens can be processed by US businesses: the EU-US Privacy Shield. US businesses are free to sign up to the Privacy Shield by promising to maintain GDPR standards in their data policies. The Privacy Shield has become the standard way in which many US and UK businesses share data; however, it does not cover businesses in the FRPS industry, a critical industry for both the UK and US. When the UK leaves the EU, it should explore whether it can agree its own Privacy Shield with the US that covers FRPS.

2. CROSS CUTTING INDUSTRY ASKS

PERSONAL DATA PROTECTION REGIMES AND PRIVACY

The ability to share without barriers and process personal data between the UK and US is vital if consumers are to benefit from the choice and competition that a digital transatlantic market can provide. At present, the UK and the US have two quite different data protection regimes, and companies operating in both markets need to operate to different standards in each country, and identify mechanisms to share personal data between them, which adds significant costs.

UK personal data regime

Existing data protection law in the UK includes restrictions on how personal data can be processed and transferred overseas. Personal data and sensitive personal data are protected by the EU's GDPR, which has been incorporated into UK law by the Data Protection Act 2018 (DPA).

- **Personal Data:** any information relating to an identified or identifiable person, such as an individual's name, address, or Internet Protocol (IP) address
- **Special Category Data:** personal data subject to enhanced protection, such as information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

The GDPR provides individuals in the EU with legal rights that are directly enforceable against organisations, including the right to access information that businesses hold about them. It also extends the scope of responsibilities for data controllers and processors, and creates an enhanced regime for enforcement which introduces the risk of heavy fines for entities found to be in breach.

Key provisions of the GDPR include:

- Enhanced transparency: data controllers are required to provide more detailed information around how data is processed, the grounds for justifying fair processing of data and the rights that individuals have in relation to their data. This means that organisations must demonstrate that they have a lawful basis for processing data. They must provide details of what information they hold on individuals, and for how long they hold the data, as well as security measures to protect individuals' rights in relation to personal data.
- Consent as a basis for processing personal data: organisations may rely on consent as a basis for processing personal data under certain circumstances. Consent in this context must be freely given, specific, informed and unambiguous, and must be confirmed by a clear statement and affirmative action. Consent can also be withdrawn, requiring companies to have another lawful basis for holding the data, should they wish to retain it.
- The requirement for a Data Protection Officer (DPO): there is a mandatory requirement to appoint a DPO where a business meets certain thresholds.
- Higher fines for data controllers and processors: organisations found to be in breach of GDPR can be subject to fines of up to €20m or 4% of the firm's global turnover (whichever is greater).

The GDPR also restricts the transfer of data from the EU to jurisdictions outside of the EU without adequate safeguards being put in place.

US position on data protection

In the US, privacy is seen as a consumer right in general and is regulated at state level (except for federal government data, for example around federal taxation, healthcare and national security). There are many state-level privacy laws which regulate the collection and use of personal data – and the number of state-level privacy laws is expected to increase over time. California is the leading US state in terms of privacy legislation, and some of its privacy laws have far-reaching effects at a national level because of the concentration of technology companies in that state. The California Consumer Privacy Act (CCPA), enacted in June 2018 and taking effect in 2020, provides consumers with several new rights, including the right to:

- require the deletion of their data
- request disclosures of information about how their personal data is collected and shared
- instruct a company not to sell their data.

It is expected that other states will follow California and implement more stringent (CCPA and GDPR-like) privacy law, but there is also tension between federal and state privacy law. Some federal and state-specific privacy laws pre-empt each other, making it more onerous for organisations operating in the US to comply with different laws regulating the same types of data – e.g. medical or health records – or the same types of activity.

The concept of a federal privacy law is building momentum and recently some of the largest tech companies in the US testified in Senate hearings in favour of a unified approach to privacy law.[12] However, there is a lack of clarity on the current administration's appetite for regulation or increased legislation in the privacy space, meaning that it is difficult for FRPS firms to plan for this eventuality.

Given the nature of US legislation, there is always likely to be a level of divergence between UK and US privacy law, and, even if it is able to do so post-Brexit, the UK currently seems unlikely to dilute current standards under the GDPR and DPA 2018. Given that overall US legislation provides a lower level of protection for the individual than UK law, the burden has been on US firms to attain the higher compliance standards in the UK.

In order to prevent a widespread fragmentation in the digital transatlantic market, governments and businesses have devised mechanisms that can be used to exchange data between the UK and US. US businesses wishing to access and process EU personal data must use either BCRs, which facilitate global movement of data within multinational businesses, or SCCs which provide adequate safeguards for data being transferred under a contract. However, these procedures can impose costly burdens on businesses, and thus can particularly disadvantage start-ups and small and medium-sized enterprises (SMEs) with the wish to provide consumers with new and innovative products.

Finally, the EU and US have devised another mechanism to address regulatory divergence: US companies can also sign up to the US Privacy Shield framework to enable cross border transfers.

EU-US Privacy Shield:

The EU-US Privacy Shield Framework was designed by the US Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States. It allows US companies to process and transfer the data of European citizens without the US government needing to secure an adequacy determination from the European Commission.

Under the Privacy Shield rules, US-based organisations are now able to transfer the data of EU citizens to the US if they self-certify to the US Department of Commerce that they will comply with the Framework's requirements on data protection. The organisation will then be deemed adequate by the EU; its commitment to abide by Privacy Shield standards is enforceable under US law.

[12] The Street, 'Google, Amazon, Apple and Other Execs Grilled on Privacy at Senate Hearings', (September 2018), available at: https://www.thestreet.com/technology/alphabet-apple-google-grilled-on-privacy-by-congress-14724966

A significant issue with the Privacy Shield is that it does not cover financial or related professional services. This is in part due to the complex regulatory environment in the US: the Privacy Shield is enforced by the US Federal Trade Commission and the US Department of Transportation, but FRPS firms are not under the jurisdiction of either of these bodies.

Once the UK leaves the EU, it will no longer be a party to the Privacy Shield and will need to devise a new way of facilitating the movement of personal data to and from the US. Regulators have been alive to the challenge and devised contingency measures to facilitate data sharing: the US Department of Commerce and the UK Information Commissioner's Office (ICO) recently issued updated guidance on how UK and US firms can continue to use the EU-US Privacy Shield post Brexit.[13] However, in the long term it would be of benefit to both countries if the UK and US could agree a new bespoke new data transfer mechanism that not only replicates but exceeds the terms of the current EU-US Privacy Shield.

Given the high levels of trust that exist between the UK and US financial regulators, it should be possible for the two countries to adapt the existing framework and agree a new mechanism that includes FRPS, providing a clear and ambitious framework for exchanging personal data between the UK and the US.

Should the UK change its personal data protection regime after Brexit?

Instead of creating new mechanisms to cater for regulatory divergence in dealing with personal data in the transatlantic market, the UK could seek to retain the GDPR standards, but address some of the bureaucratic and other elements of the GDPR, which do not result in the desired outcome. After Brexit, the UK may have the ability to move away from the GDPR framework, and there are some who argue that moving to a more US style, 'light touch' personal data regime would remove barriers to entry for technology businesses, spur innovation and reduce business operating costs.[14] But there are several reasons to currently expect that the UK will continue to align closely to GDPR after Brexit:

- It would allow seamless trade with Europe, its biggest trading partner.[15]
- If the UK changed its data protection policy, any UK business wishing to do business with EU citizens would still have to comply with GDPR standards, creating a two-tiered system.
- Businesses have already devoted considerable resources to adopting GDPR standards (including many based in the US), with many technology businesses having adopted GDPR globally, given that the GDPR provides a very high standard/global standard of data protection.
- If the UK moved away from GDPR, it would risk not achieving an 'adequacy' status, meaning that UK businesses would suffer serious disruptions with the EU.
- Strong personal data protections are increasingly seen as a business and societal benefit in the UK, and not something that could be traded away by a government without provoking a strongly negative reaction from the electorate and business.

It is unlikely, therefore, that the UK would move to dilute its Data Protection regime, either generally or in relation to FRPS. An enhanced Privacy Shield-type mechanism that covers FRPS offers a more pragmatic route forward.

Industry ask

The UK and US should negotiate a new Privacy Shield that includes FRPS. This would give US firms committing to the Privacy Shield certainty that they could transfer UK data within their organisation, and UK firms confidence that data transfers to the US would be compliant with UK Data Protection principles.

[13] 'No-deal Brexit' in this Report refers to the UK and EU not agreeing the draft 'deal' before the 31 October 2019. In this event the UK government will not have ratified the WA and Political Declaration under the procedure set out under s.13 of the EUWA.

[14] TechUK, 'Written evidence submitted by TechUK', (January 2018), available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/international-trade-committee/ukus-trade-relations/written/77394.html

[15] The EU, taken as a whole is the UK's largest trading partner. In 2017, UK exports to the EU were £274 billion (44% of all UK exports). UK imports from the EU were £341 billion (53% of all UK imports) - House of Commons Library, 'Statistics on UK-EU trade', (July 2019), available at: https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7851

CHALLENGING DATA LOCALISATION

Around the world, governments are engaging in battles over data localisation measures, which require organisations to store certain types of data on servers within certain borders. Under such controls, organisations are prevented from transferring relevant data externally or to branches based in other countries, or storing the data on an international server. China is one example of a jurisdiction that has implemented a regulatory framework of forced data localisation; other countries have introduced barriers, to varying extents. The US, and, to a lesser degree, the EU, allow the free flow of cross-border data, subject to limited restrictions.

The US and the UK are strong advocates of free data movement, and have a record of resisting localisation requirements when possible. However, an increasing number of countries, led by China, are adamant that there is a need for countries to impose localisation requirements. Many argue that some restrictions on data processing and international data transfers are necessary, and have been implemented to protect consumers. Such arguments are often made with respect to financial services, on grounds such as the maintenance of financial stability or the need for data to be available to regulators.

A number of recent trade agreements have tried to tackle localisation requirements. As the UK and US are both strongly sceptical of the rationale for localisation, there is significant potential for them to work together to craft an agreement with unprecedented restrictions on localisation. At a time when some markets are moving away from free data movement, an ambitious agreement between the world's two largest international financial centres on limiting data localisation in financial services could help set global standards in a pro-free trade direction, and provide a model for what trade agreements can achieve on digital trade.

UK-US alignment on localisation

The UK government position on localisation is clear. It believes that "data localisation has many negative consequences", importantly that it "risks weakening data security, (…) can lock out SMEs and new market entrants, stifle competition and undermine the take-up of cloud computing services".[16] The UK government has also stated publicly that it considers data localisation "anti-competitive and `contrary to Single Market principles", although, similarly to the US approach, it has shown limited support for some data localisation in respect of UK citizens' public NHS health records and tax information. There are however instances where the FCA feels that localisation of data is justified - for example, in relation to national security and carrying out law enforcement activities.

Separate to this, the FCA has expressed concern that restrictive domestic rules could lead to market fragmentation, which restricts the free-flow of financial services activity and therefore has the potential to reduce liquidity, increase fragility and reduce operational efficiencies.[17]

The US position is similar to that of the UK on data. The US has been a world-leading advocate in fighting localisation measures through trade policy. According to a US International Trade Commission report, US industry representatives stated that while there are many types of data protection measures, data localisation was the most severe barrier to digital trade.[18] This perspective is clearly reflected in the USMCA, which includes a provision that prevents the US, Mexico or Canada from requiring businesses to use or locate computing facilities in their local jurisdiction,[19] and an outright ban on data localisation (including in financial services), except in very clearly delineated circumstances. Meanwhile, the US Commodity Futures Trading Commission's (CFTC) strategy has clearly set itself against localisation in financial services, instead suggesting that prudential issues be dealt with through efforts to "examine response procedures to cyber incidents and update data retention best practices", rather than looking to data localisation.[20]

[16] European Commission, 'UK government response to the European Commission's consultation on building the European data economy', (2017), available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-30/consultation_data_eco-uk_653FBCB9-F30C-9431-7A77F4C6C08AF57B_46171.pdf

[17] The Financial Conduct Authority, 'Brexit and Beyond', (March 2019), available at: https://www.fca.org.uk/news/speeches/brexit-and-beyond

[18] United States International Trade Commission, 'Global Digital Trade 1', (August 2017), available at: https://www.usitc.gov/publications/332/pub4716.pdf

[19] United States-Mexico-Canada Agreement, 'Financial Services', (August 2019), available at: https://usmca.com/financial-services-usmca-chapter-17/

[20] U.S. Commodity Futures Trading Commission, 'Statement of CFTC Commissioner Dawn D. Stump on Data Protection Initiative', (March 2019), available at: https://www.cftc.gov/PressRoom/SpeechesTestimony/stumpstatement030119

The economic impact of data localisation

Data localisation requirements act as a barrier to entry, given the additional costs, and the effect on small businesses and start-ups could prove detrimental to innovation. Strict requirements can also be harmful to major international technology businesses, if significant additional cost is introduced as a result.

Overall, the economic impact assessment of data localisation is significant. The European Centre for International Political Economy (ECIPE) found that globally, data localisation laws could drain between 0.7% and 1.1% of GDP from the economy.[21] However, it is estimated that the removal of data localisation restrictions would result in combined annual GDP gains for EU Member States of up to €8bn (£6.82bn).[22] When considering these figures, it should be noted that the costs associated with localisation are not restricted to visible costs – there are also hidden long-term opportunity costs, such as depriving economies of the benefit of valuable FinTech initiatives.

It is also important to note that in the context of financial services, localisation measures (or, indeed, any restriction on cross-border data flows) can increase financial stability risks by making it harder for home-country regulators to understand what is happening to the balance sheets of banks they are responsible for regulating who have a presence in host countries with localisation requirements.

As the Global Financial Markets Association has argued, "data localisation policies can prevent financial regulators from having the data necessary to do their jobs effectively, as well as undermine firms' efforts to comply with regulatory requirements."[23] For example, localisation policies can make it harder for financial institutions to share information with their international affiliates to obtain information necessary to file suspicious activity reports (SARs) under anti-money laundering regulations.

An early illustration of how home regulators can respond to data movement restrictions in foreign markets can be found in the decision of the SEC to refuse to register EU-based asset managers effectively preventing them from raising funds in the US. This happened because the SEC is concerned that the restrictions on data sharing, which has been further limited by GDPR, would prevent it from being able to obtain data from the asset managers in question.

There are clear economic costs associated with data localisation, but localisation advocates believe that some of these costs are worth paying in return for enhanced consumer protection. China, Turkey and Russia have implemented a perceived regulatory framework for data localisation, and Brazil, India, Indonesia, South Korea, and Vietnam have all begun to introduce regulatory barriers enforcing data localisation (as outlined in the Appendix). For most of these countries, concern for protecting citizens' personal data has been the reason cited to justify the introduction of regulatory barriers. Some governments believe having greater control of citizens' personal data will help prevent misuse, provide regulators with ready access, support local employment and safeguard consumer interests, which is a concern in relation to information held by public sector entities (e.g. health records and tax data). Additionally, following the revelations of global surveillance programmes, some governments and regulators feel that data localisation could protect against foreign cyber attacks, and could have wider benefits for domestic cloud computing industries, as local IT firms build infrastructure to support cloud-related business requirements.

[21] The European Centre for International Political Economy, 'The Costs of Data Localisation: A Friendly Fire on Economic Recovery', (May 2014), available at: http://ecipe.org/publications/dataloc/

[22] UK Parliament, 'Digital Single Market: Building a European Data Economy', (March 2017), available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmeuleg/71-xxxii/7107.htm#footnote-055

[23] ASIFMA, 'Data Localisation - GFMA's Data Privacy, Security and Mobility Principles', (April 2019), available at: https://www.asifma.org/wp-content/uploads/2019/07/asifma-letter-on-gfma-data-mobility-principles-f20190418.pdf

Alternative measures to localisation requirements

Although the economic case against localisation seems strong, it is important to consider the security and right-to-access reasons advanced by many regulators to justify implementing data localisation laws. In April 2018, the Reserve Bank of India (RBI) issued a new rule for payment systems providers operating in the country – under the rule, all data on payment system users collected within India must be localised within six months. The RBI said it was motivated by the need to have "unfettered supervisory access"[24] to such data, given the fast-growing and increasingly technology dependent payments ecosystem in India. Despite such concerns, in practice the cloud can be set up to be just as secure as on-premise solutions. In the private sector, entrusting data to dedicated outsourced cloud providers that are focused on protection may even provide increased security, better data audit trails and more flexible infrastructure capacity.

Industry ask

One possible solution that would allow regulators to access data without requiring localisation barriers to be imposed on trade would be for governments to allow trusted third-party data-brokers (sometimes referred to as database marketers or consumer data analytics firms) to develop application program interfaces (APIs) that permit regulators to access data if specific circumstances are activated. Data brokers would maintain records of trades, for example, with all personal data anonymised and there would be policy enforcements to prevent data movement in certain pre-specified circumstances

Summary view on localisation

Although data localisation is a complex issue, it would be in the commercial interests of both the UK and the US to agree a comprehensive prohibition on data localisation requirements across FRPS (as in USMCA and in the USTR's published negotiating objectives for the UK). Although there may be a legitimate need for exceptions allowing limited localisation for prudential reasons, it is urged that such exceptions be very clearly defined, as in the USMCA.

If the UK and US reach an ambitious agreement on data localisation, in addition to immediate commercial advantages, there would be considerable long-term benefits. Currently, many countries are imposing localisation requirements on financial services, causing fragmentation in the global market. Now is an opportune time for the two leading liberalising powers in global financial services to shape a new framework on data localisation that strikes the right balance between maintaining open digital markets, ensuring the highest possible standards of data protection, and keeping essential prudential powers in the hands of domestic regulators.

[24] The Reserve Bank of India, 'Storage of Payment System Data', (April 2018), available at: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0
[25] Forbes, 'Marriott Breach Exposes Far More Than Just Data', (December 2018), available at: https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#7d0ba4596297

Improving national security and tackling cyber and financial crime

Over the last decade, large-scale cyber attacks have become more common and hackers have obtained access to government databases around the world – the case of Edward Snowden and WikiLeaks being a high-profile example. Major corporations' information systems have also been breached because of hackers performing sophisticated attacks on a massive scale, as was seen in the 2018 Marriot International breach.[25]

In the context of data protection and cyber security, regulatory cooperation could help establish a framework for identifying and collaborating to prevent and address cyber-security-related incidents and the attempted misuse of digital data. This would lead to increased protections for customers and businesses, and help increase confidence in e-commerce on both sides of the Atlantic.

Cooperation of this nature has been achieved in the past. Under the Five Eyes programme, the UK, US, Canada, Australia and New Zealand have already created a platform for information sharing and surveillance for security purposes. Five Eyes was developed in the Cold War, and has established a precedent for strong collaboration between the UK and US on information sharing. Today, the programme serves as a model for how the two countries could further develop trust and understanding.

Going forward, any framework for regulatory coherence on cyber issues must define clearly how responsibilities are allocated to regulatory and security bodies, and determine what legal precedents will apply in the event of a cyber security breach. Both partners would need to agree on the relevant jurisdiction, settlement and enforcement provisions where there is a cross-border incident, and there may be scope for new UK-US regulatory and security bodies to be established for this purpose.

REGTECH

RegTech involves the use of technology to manage regulatory processes primarily within the FRPS industry. The main functions of RegTech include regulatory monitoring, reporting, and compliance: RegTech companies use cloud computing technology to help businesses comply with regulations more efficiently and at lower cost.

RegTech remains largely uncharted water for both firms and regulators, although some regulators are already leveraging new technology and analytics to better identify and manage systemic risk by analysing data collected from regulated firms. RegTech has an important part to play in helping overcome difficulties that firms face around regulatory divergence. Although it would be challenging to seek to fully reverse the trend towards regulatory divergence between the US and EU that set in following the financial crisis of 2008, RegTech could act as a bridge to counter such divergence by making it easier for firms to navigate the different approaches and reducing compliance costs.

Regulators can also use RegTech to assist them in their efforts to combat money laundering and financial crime. Regulators in the UK and US have recognised that RegTech can facilitate data and knowledge sharing among relevant bodies which helps them identify and impede complex criminal networks.[26] In an example of a positive initiative, the FCA hosted the 2019 Global AML and Financial Crime TechSprint, where they worked with US and other international regulators to explore issues such as:

- How can a network of market participants use privacy enhancing technologies and data analytics to interrogate financial transactions stored in databases within institutions to identify credible suspicions without compromising data privacy legislation?
- How can market participants efficiently and effectively codify typologies of crime which can be shared and readily implemented by others in their crime controls?
- How can a market participant check that the company or individual they are performing due diligence on hasn't raised flags or concerns within another market participant, and/or verify that the data elements they have for the company or individual match those held by another market participant?
- How can technology be used to assist in identifying an ultimate beneficial owner across a network of market participants and a national register?[27]

Initiatives such as the TechSprint demonstrate the effectiveness of regulatory cooperation around data, and regulators should be on the lookout for similar opportunities to use new technology to promote key regulatory goals.

[26] The Financial Conduct Authority, 'Global AML and Financial Crime TechSprint', (March 2019), available at: https://www.fca.org.uk/events/techsprints/aml-financial-crime-international-techsprint
[27] Ibid.

3. SECTOR-SPECIFIC EXAMPLES

Many sectors within the FRPS industry face barriers and restrictions when it comes to sharing data between the UK and the US. As the UK government considers how to tackle some of these barriers, this section of the report aims to outline some of these sector-specific restrictions and detail some potential solutions and propositions. Not all of these barriers require government-to-government action to unblock them; some breakthroughs can be facilitated by industry-to-industry dialogue; others by regulator-to-regulator dialogue. In order to ensure a coordinated approach from the UK towards improving trade in data with the US, therefore, it will be essential that government, regulators and industry work closely together.

Payments

The growth of the international payments industry is becoming increasingly contingent on technology and the free flow of data. Between 2015 and 2016, global non-cash transaction volumes grew two-fold resulting in a total of $482.6bn.[28] In 2016, 66.3% of the global market share in non-cash transactions was linked to mature markets, including the UK and US.[29] However, the trend is for market share to move to emerging markets.

Over the last 10 years, more developed markets have lost around 20% of their market share to developing markets and it is expected that China will overtake the US as the largest market for non-cash transactions by 2021.[30] Businesses in the UK and US should therefore consider how they can use technology and the sharing of data to retain market share.

The UK is at the forefront of innovation in the payments industry in terms of efficiency of payment services, security for customers and potential for increased competition. The US, on the other hand, does not have the same infrastructure to support faster payments or the technology to authenticate payments and allow new market players to interact with existing financial services participants.

When making an online payment in the UK, a UK payee can expect to receive the funds in their account within a few days and in many cases instantly.[31,32] The process takes longer in the US; the US recently established a 'US Faster Payments Taskforce' to devise a strategy for implementing "safe, ubiquitous, faster payments".[33,34] Clearing House, which is a banking association and payments company that operates much of the core payment systems infrastructure in the US, has also since launched a real-time payment system for all US banks called 'RTP'. It is anticipated RTP in conjunction with the use of APIs will allow for this part of the US financial services sector to develop and innovate.[35]

The lag in development on the US payments side arguably affects overall transaction times for UK-US cross-border payments. Cross-border transactions are almost exclusively handled by banks through correspondent banking where local banks carry out transactions on behalf of foreign banks without a local presence.[36] The global banking share of this cross-border market in business-to-business (B2B) and business-to-customer (B2C) transactions is more than 95%.[37] The WTO considers that Tier 1 banks "have a monopolistic share of this market segment because of the extensive regulatory compliance framework…,

[28] Capgemini, 'World Payments Report', (October 2018), available at: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf
[29] Ibid.
[30] Ibid.
[31] Within the UK, BACS acts as an electronic system that enables customers (usually organisations) to transfer money from one bank account to another within three working days.
[32] Within the UK, Faster Payments and CHAPS are online payment services that can be used to transfer money into a payee's account on the same day. For Faster Payments, the payment will arrive in the payee's account almost immediately (or within two hours) as long as the payee's bank or building society uses Faster Payments. CHAPS, on the other hand, guarantees that funds will be paid into a UK account on the same day as long as the payer makes the payment online before 17:00.
[33] Faster Payments Taskforce, 'Goals and recommendations', (August 2019), available at: https://fasterpaymentstaskforce.org/goals-and-recommendations/
[34] US Federal Reserve System, 'Strategies for Improving the U.S. Payment System', (January 2015), available at: http://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf
[35] Go Medici, 'The Road to Faster Payments in the US', (December 2018), available at: https://gomedici.com/road-to-faster-payments-in-the-us/
[36] McKinsey & Company, 'Payments', (June 2016), available at: https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Rethinking%20correspondent%20banking/Rethinking-correspondent-banking.ashx
[37] Ibid.

lack of alternatives and the cost of maintaining large correspondent banking relationships".[38] As a result, cross-border B2B transactions are around 10 times more expensive for bank customers than domestic transactions.[39]

Industry ask

The UK and US should work together on greater interoperability between payment systems and the authorisation of entities' access to these systems as well as the standards such as ISO20022 which underlie and support instant payments.

The US should also actively consider the access of non-bank entities to payment systems.

As an alternative, UK and US customers can use SWIFT payments via the SWIFT international payment network, ensuring the funds (regardless of currency) reach the payee's account within one to three working days.[40] While SWIFT has proven efficient for UK and US users seeking to transfer money internationally, UK and US regulators and trade negotiators could help identify ways to enhance international money transfer schemes between the UK and US. In such efforts, the objective should be to improve overall transaction times and security, and allow for more financial services entities other than banks to compete in the money transfer services market.

Strong Customer Authentication

The UK is at the forefront of customer authentication in financial services, in part because of high quality regulation set out in the Payment Services Regulations 2017 (which implements the Second EU Payment Services Directive in the UK) and the Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common Secure Communication (CSC).

While there are some exemptions to SCA for low-risk and low-value payments, US banks and payment service providers need to meet the SCA requirements if they wish to operate in the UK. The US should consider adopting a similar level of protection for its online customers not only to allow for more frictionless payment services in the US but also to enable more cross-border payments between UK customers and US-based e-commerce platforms.

Industry ask

The US government should agree to implement requirements for its banks and payment services providers to adopt three factor authentication so the US can provide its customers with the same level of protection provided to UK customers. This might open the US market to more business from UK customers and will also allow for more US businesses to operate in the UK in compliance with SCA.

The UK and US might consider sharing some of the data where payments cannot be authenticated to help monitor cross-border fraud and tackle financial crime.

[38] World Trade Organization, 'The economics of how digital technologies impact trade', (October 2018), available at: https://www.wto.org/english/res_e/publications_e/wtr18_3_e.pdf

[39] More specifically, the banks' revenue margin on cross-border transactions is 20% as compared to 2% on domestic transactions. The revenue calculations include transaction fees, float income and foreign exchange fees – McKinsey & Company, 'Payments', (June 2016), available at: https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Rethinking%20correspondent%20banking/Rethinking-correspondent-banking.ashx

[40] TransferWise, 'What are SWIFT payments', (August 2019), available at: https://transferwise.com/help/article/1663580/paying-by-bank-transfer/what-are-swift-payments

Open Banking

Open Banking aims to foster competition and encourage innovation by requiring participating banks to share customers' data (where the customer consents) including performance and fee data, with third party financial services providers. This will make it easier for customers to compare various products and services across participating banks, FinTech providers and non-bank members.[41] It is resulting in an industry shift with new types of banks and financial services businesses beginning to compete in the UK financial services market, as is the case with digital banks N26 and Fidor and digital lender Klarna which are of EU origin.[42]

Open Banking is a strong example of how digital innovation has the potential to liberalise the UK-US retail banking markets. The US financial services sector is also seeing a shift with US banks entering into data-sharing agreements with financial services businesses.[43] For instance, Chase's partnership with Intuit and Wells Fargo's partnerships with Xero and Finicity.[44] The US banks have been using APIs for several years to allow personal financial management software to operate as well as providing developers with a platform to interact with payment networks. However, unlike in the UK, APIs in the US have mainly been established to share customers' financial information rather than being used to initiate payments or transfer funds.[45]

Open Banking

Open Banking is a UK government-led initiative set up by the Competition and Markets Authority (CMA). Its intention is to increase competition and innovation in the UK financial services market by requiring the participating banks (referred to as the CMA 9) to allow third party providers (TPPs) to make use of application programming interfaces (APIs) so they can access customers' financial data and provide additional financial services. Customers will be able to benefit from account information services to better understand their spending habits (similar to some of the functionalities provided by Monzo), and will be able to easily transfer money through payment initiation services.

Industry ask

US regulators should consider rolling out a similar open banking initiative to allow for UK TPPs to enter the US market and US TPPs to expand into the UK, and to allow for UK customers to benefit from Account Information Service (AIS) and Payment Initiation Service (PIS) on a cross-border basis. This would not only enhance e-commerce but also ensure there are the same standards of protection for customers seeking to make payments through US websites. As a preliminary step, the UK government should consider how to encourage the US to adopt such regulation: proposing the formation of a UK-US working group to exchange insight and best practice on Open Banking might be a helpful starting point.

[41] Forbes, 'Why Big UK Banks Are Worried About Open Banking', (March 2018), available at: https://www.forbes.com/sites/baininsights/2018/03/15/why-big-uk-banks-are-worried-about-open-banking/
[42] McKinsey & Company, 'Data sharing and open banking', (September 2017), available at: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking
[43] Ibid.
[44] Ibid.
[45] Ibid.

Consumer credit

The sharing of consumer credit history provides opportunities for the UK and US to work together to tackle financial crime and facilitate cross-border market access. At present, UK customers relocating to the US are likely to face difficulties in securing credit or buying another financial services product where they cannot prove affordability with a US credit history. For instance, where a credit reporting agency lacks sufficient data on a loan applicant and is unable to generate a credit score, then it is unlikely the applicant will be successful. The same applies for US customers who move to the UK. Creating a series of APIs between major credit reporting agencies including Equifax, Experian, TransUnion and Callcredit might allow for customers who are not a credit risk and might have data stored in the other jurisdiction to obtain a loan or other form of credit more easily. It would also allow more oversight by credit reporting agencies over the two markets, increase the rate of domestic (and perhaps cross-jurisdictional) borrowing and result in fewer bad loans.[46] The UK and US might also consider creating a blockchain to store this sort of information and allowing users to transport their own credit history data between jurisdictions and giving access to credit agencies depending on the products they are seeking to buy.

Industry ask

A commitment between the UK and US' approved credit reporting agencies to share customers' credit information (with their consent) to facilitate lending on a cross-border basis and meet the banking needs of recently arrived expatriates. This will have wider benefits for the UK and US financial services markets and enhanced transparency around customers' affordability could lower financial risk taking. The UK and US to consider how blockchain technology might help users moving between the two countries transport their data.

Supporting innovation in payments and banking

Noting the recent establishment of a Financial Innovation Partnership between the US Treasury and HM Treasury which exists to deepen bilateral engagement on regulation in financial technology, the FCA and the SEC could consider partnering to create a joint regulatory sandbox to help banks with a digital offering to operate in both jurisdictions. This could draw on the sandbox set up by the European Commission for Financial Stability, Financial Services and Capital Markets Union which on 2 April 2019 launched its European Forum for Innovation Facilitators (EFIF). This intends to harmonise and align practices of EU Member States with regard to existing innovation and regulatory sandboxes as well as the existing FCA, US SEC and ICO sandboxes, enabling FinTechs to scale up in the single market. Harmonisation might not be an appropriate goal for UK-US regulatory cooperation, given regulators' desire to preserve autonomy. However, sharing ideas about how to approach these issues might form a basis for mutual recognition at a later stage. The UK and US might also want to establish a body to review both markets, share information on FinTech development and detect any regulatory issues at an early stage.

Industry ask

Commitment by both parties to support cross-border innovation in financial services and enable traditional banks to participate in regulatory sandboxes alongside smaller FinTech firms.

[46] Center for Data Innovation, '10 Steps Congress Can Take to Accelerate Data Innovation', (May 2017), available at: http://www2.datainnovation.org/2017-data-innovation-agenda.pdf

Asset management

The UK and US asset management sectors already benefit from strong commercial bilateral ties, although the market that particular asset management firms operate in is often localised rather than purely cross-border. In practice, for retail and so-called 'mutual' funds, market structures and, in particular, the respective tax regimes mean that it is rare for US funds to be sold to non-US citizens, or for UK firms to sell UK funds to US clients. Major firms have established local operations and operate through separate legal entities in the US and the UK and/or EU. In the sphere of alternative funds for institutional investors, private placement regimes and certain US exemptions enable a level of cross-border business to take place. Often, international fund management businesses establish structures whereby funds are operated by one entity (established in the US or UK and regulated under those rules), which appoints a group entity in the other country either as a sub-advisor, sub-manager, service provider, distributor or delegee. Such arrangements work well in practice and current rules governing data flows do not create a significant impediment to their operation between group or non-group companies in the two countries.

The respective tax rules in the UK and the US make UK retail buying of US funds largely unattractive, and vice-versa (for example, UK customers would have to pay capital gains on unrealised profits in the US). In addition, US retail investor protection rules tend to prioritise US citizens over non-US citizens which dilutes enthusiasm from UK wealth and asset management firms to prioritise increasing cross-border market access.

Increased regulatory cooperation around asset management could help businesses on both sides of the Atlantic. The cross-border funds market could benefit from increased data sharing between UK and US regulators. Both regulators already have considerable data about the sector at their disposal. On the UK side, since the introduction of the EU Markets in Financial Instruments Directive II (MiFiD II) and Markets in Financial Instruments Regulation (MiFIR),[47] which came into force on 3 January 2018[48] the FCA has processed over 30 million transaction reports per day, and currently shares around 70% of these transaction reports with other EEA national competent authorities.[49] Many US hedge funds, asset managers and buy-side and sell-side fund managers rely on the data to prevent market abuse, and to consider trends in the UK market that might carry over to the US.

[47] (1) MiFiD II – Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance; and (2) Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 Text with EEA relevance (also known as MiFiR).

[48] MiFiD II was required to be transposed into UK law by 3 July 2017, and MiFIR had direct effect as an EU Regulation. MiFiD II was transposed into UK law by way of various UK implementing legislative instruments, including ; (1) The Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) Order 2017 (March 2017); (2) The Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) (No. 2) Order 2017 (March 2017); (3) The Financial Services and Markets Act 2000 (Markets in Financial Instruments) Regulations 2017 (June 2017); (4) The Financial Services and Markets Act 2000 (Markets in Financial Instruments) (No.2) Regulations 2017 (December 2017); and (5) The Data Reporting Services Regulations 2017 (June 2017).

[49] The Financial Conduct Authority, 'EU Withdrawal Impact Assessment', (November 2018), available at: https://www.fca.org.uk/publication/impact-assessments/eu-withdrawal-impact-assessment.pdf

Access to accurate data is crucial for the management of funds and for risk management. For example, the Alternative Investment Fund Managers Directive (AIFMD) requires that in maintaining safeguards against conflicts of interest, "decisions taken by the risk management function are [to be] based on reliable data".[50] Given that many US hedge fund managers participate in the UK-US wealth and asset management market, data processing remains a key consideration for any future UK-US regulatory discussions concerning the sector.

There might be scope for UK and US fund managers to agree to develop a platform or API for sharing high level data which might impact industry level or regulatory decision making, and help ensure that UK and US regulators make decisions and policies based on the same data.[51]

Industry ask

Secure agreement from wealth and asset management market participants in UK-US to share market data in support of increased market transparency and to inform regulation. The UK and US would need to agree a set of principles and legal rules for the formation of the platform (API) or database, determining which types of firms would need to contribute.

[50] The Financial Conduct Authority, 'Requirements for alternative investment fund managers - section 3.7.4', (august 2019), available at: https://www.handbook.fca.org.uk/handbook/FUND/3.pdf

[51] United States-Mexico-Canada Agreement, 'Financial Services - Section 17.12(2)', (August 2019), available at: https://usmca.com/financial-services-usmca-chapter-17/

Insurance

The UK insurance sector is the fourth largest in the world; and total UK insurance premium volume accounted for a 6.5% share of the world market in 2018.[52] In 2015, the UK exported circa $4bn of insurance and pensions services to the US whilst importing £146m from the US.[53] Data sharing between UK and US insurance providers presents a significant opportunity to develop a wider range of insurance products, to identify where there may be any gaps in the market and to find instances where a customer might be better suited to another product. Data sharing could pave the way for better collaboration around innovation for both countries.

- **Covered Agreements:** an example of EU-US market liberalisation.

  The EU-US Covered Agreement helps to level the regulatory playing field for US insurers and reinsurers operating in the EU and allows US insurers with EU operations to avoid burdensome worldwide group capital, governance and reporting requirements under the EU's Solvency II prudential regulatory system for insurers.

- **The covered agreement addresses three areas of insurance and reinsurance prudential measures:**
  - group supervision
  - reinsurance supervision, including collateral and local presence requirements
  - exchange of information between supervisory authorities.

The UK-US Covered Agreement, agreed in December 2018, essentially replicated the provisions of the EU-US Covered Agreement.

Industry ask

The US and UK should agree to evaluate the 'US-UK Covered Agreement' after it comes into effect and after two years assess its effectiveness in achieving its overall intentions of enhancing regulatory certainty and market continuity. If it is seen to fall short, the UK and US should agree to address any inconsistencies or gaps by aligning regulation and for instance, agreeing to allow UK insurers to be considered 'foreign' rather than 'alien' firms under US insurance regulation.

[52] Swiss Re, 'Sigma 3/2019: World insurance: the great pivot east continues', (July 2019), available at: https://www.swissre.com/institute/research/sigma-research/sigma-2019-03.html

[53] Association of British Insurers, 'Submission to the International Trade Select Committee inquiry: UK-US trade relations (TER0019)', (November 2017), available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/international-trade-committee/ukus-trade-relations/written/73927.html

Cyber insurance

Since around 2013, cyber risk has become a leading global risk for businesses and large scale cyber-attacks were within the top five global risks in terms of likelihood for 2017 and 2018 according to the World Economic Forum.[54,55] Cyber insurance is an exciting growth area for both the UK and the US; at present, much of the wording in some traditional insurance policies (i.e. non-cyber insurance products) is not explicit on cyber related losses. One of the biggest challenges the insurance industry faces is around the ability to model potential cyber-related losses, particularly due to the potential for the accumulation of multiple losses from a single attack, and therefore how to accurately price cyber risk. Uninhibited free flow of data will be a material component to the continued growth of the global cyber insurance sector, particularly post-Brexit.

It is in the interests of the US and the UK that the cyber insurance market continues to flourish and that these key players are at the cutting edge. The UK government believes that "technological innovation will allow insurers to monitor customers' behaviour with more precision, and insurance premiums can be more accurately tailored to individual characteristics".[56] Such technological developments would benefit insurers in both wholesale and retail spheres, but insurers will need to have arrangements in place which facilitate their access to the relevant data. Insofar as insurers are able to harness data to build better tailored products and services, they will need to meet the legal requirements of the jurisdictions in which they are operating, and anticipate being held accountable for their actions regarding data.

Industry ask

Bilateral focus on the need to develop and expand the cyber insurance market on a cross-border basis not just for businesses but also for individuals. Consideration should be given to exploring where regulatory alignment between the UK and the US could help provide mutual benefit to growth.

Industry ask

Investment by the industry in both counties should be undertaken, to support the expansion of the cross-border cyber insurance industry between the UK and the US. The FCA should explore with relevant regulators in the US states and with the largest insurance providers whether an MoU would offer an effective basis for sharing data on cyber insurance, for the benefit of better understanding the types of insurance products to be marketed to businesses and individuals. A working group drawn from the industry and regulatory bodies could help to establish the mutual benefits of sharing cyber claims experience and how enhanced user access to data on cyber breaches may help to improve underwriting and exposure management.

Industry ask

There should be a joint UK-US industry initiative to encourage cyber insurance consumers to offer insurers enhanced details of the data they wish to insure, in the interests of improved product development and to allow the design of insurance policies tailored to specific needs. This should be matched by commitments from both UK and US regulators bodies to hold insurers accountable for their approach to protecting and analysing such data, with strict enforcement in cases of breaches of data protection legislation or of the terms on which insurance consumers provided information. A balance of this kind will be essential to give consumers the confidence to share their data. If achieved, it could lead to better identification of gaps in cybersecurity, improved definition of areas requiring the establishment of new bilateral rules for data-sharing, and some consequent product innovation in cyber insurance itself.

[54] European Insurance and occupational pensions authority, 'Understanding Cyber Insurance', (August 2018), available at: https://eiopa.europa.eu/Publications/Reports/EIOPA%20Understanding%20cyber%20insurance.pdf

[55] World Economic Forum, 'The Global Risks Report 2018', (January 2018), available at: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[56] Minister for Digital Matt Hancock's address to the Association of British Insurers' Conference, 'Insurance in the Digital World', (October 2017), available at: https://www.gov.uk/government/speeches/insurance-in-the-digital-world

Accountancy, audit and legal services

The financial services sector could not function without the support of a range of related professional services, such as legal services, management consultancy, accounting and audit. As UK-US data exchange for the FRPS industry as a whole increases, it will be vital to consider the interests of the accountancy, audit and legal services sectors.

Legal services

In legal services, digital continues to transform the way legal databases are managed through enabling easier access to legal resources, case precedent and commentary. There are already legal resources available to access consolidated information about UK and US legal systems, cases and academic journals, however, technology and digitisation have the potential to collate and analyse material at a much quicker pace.

At a business level, RegTech is being used to view, extract and analyse data to improve overall efficiency in law firms and for in-house teams.[57] Large amounts of information can be stored electronically on a digital portal and multiple users can access and edit the information – incredibly useful for large scale matters where there are several parties involved (for instance in dispute resolution and corporate transactions). RegTech can also help improve overall transaction time as relevant material is available almost instantaneously, where previously it might have been transferred in hard copy or stored across multiple electronic locations. New types of software are being used to carry out document review, contract review and to produce smart contracts, lowering overall costs for firms and their clients, and there is scope for this sort of material to be stored using Blockchain technology, with each user or body having their own unique access code to obtain data.

The UK government has put together an industry-led group of experts and leading figures from government and the judiciary to provide direction to the legal sector and help foster an environment in which new technology can thrive. The LawTech Delivery Panel works with industry, government, experts and the legal community, addressing challenges related to regulation, investment and funding, education and skills, legal framework, commercial disputes resolution and ethics. There is scope for this group to collaborate with relevant US stakeholders to promote digital trade and UK-US regulatory cooperation on LawTech.

Accountancy and audit services

Data is not an inhibitor to the audit/accounting business in the same way as it is for the other FRPS sub-sectors but there are areas where wider sharing of data would contribute to enhanced audit quality, such as greater access for businesses to prudential regulatory data, which would help to restore trust in audits, benefitting financial services more broadly.

Another issue concerning audit and accounting relates to the delineation between personal and business data. In practice, the individuals involved in the free movement of data have experience in business and a good understanding of data and risk, which mitigates potential issues. However, governments and businesses should take steps towards aligning the definitions of these types of data given the risks of confusion around data flows particularly where high net worth individuals are concerned.

Where an audit firm is operating in both the UK and the US, there are clear benefits in allowing prudential regulatory data to be shared on an international basis. It is important to consider that firms would need confidence that independence was not being compromised in the process. Therefore the best course of action would be for US and UK prudential regulators to reach an agreement on where to draw the lines in relation to this access. A good first step would be to establish a committee for this purpose, or to generate discussion through an appropriate forum.

[57] EY, 'How can regulation keep up as technological innovation races ahead?', (August 2018), available at: https://www.ey.com/Publication/vwLUAssets/ey-how-can-regulation-keep-up-as-technological-innovation-races-ahead/$File/ey-how-can-regulation-keep-up-as-technological-innovation-races-ahead.pdf

In terms of the specifics of how increased access to data could support the sector, businesses would benefit if prudential regulatory data could be anonymised and made available for audit firms to create trade logs, loan registers, Derivatives and Repo Clearing, loan credit quality ratings, bankruptcy and credit ratings (SME), and collate data from clearing houses to facilitate quicker data driven audits. Data from groups of companies could be pooled, as is the case with Open Banking, which allows data to be shared on a pooled and individual basis – although note that in Open Banking the transfer of data is restricted even though free sharing would benefit businesses.

Another option in terms of accessibility of prudential regulatory data would be to allow audit committees and audit chairs to have access to the data – independent audit chairs and audit committees would be able to look at and assess the risk of the companies going forward, without this information being shared across the entire board.

Industry ask

Establishing a working group for UK and US professional services bodies (e.g. the UK Solicitors Regulation Authority and the Audit, Reporting and Governance Authority amongst others, and their equivalents in the US) to discuss how the sharing of data on a cross-border basis would benefit their respective industries and allow for more bilateral market development. Consideration of how blockchain could be used to better store data.

Industry ask

Consideration of the development of an API to share relevant legal information, namely case precedent to provide insight to the courts, law firms and relevant organisations with legal practices in both countries, as well as to help businesses that are operating on a cross-border basis understand any legal requirements that may impact them. This API would act as a knowledge tool to the legal sector in both countries.

Industry ask

Development of a separate API to be managed and run at government level containing key information needed for auditing of businesses operating on a cross-border basis. The API would include firewalls to maintain independence where necessary. It would also include a separate portal of anonymised prudential regulatory data to allow audit firms to create trade logs, loan registers, Derivatives and Repo Clearing, loan credit quality ratings, bankruptcy and credit ratings (SME), and collate data from clearing houses to facilitate quicker data driven audits.

4. EVIDENCE BASE AND SUMMARY INDUSTRY ASKS

Summary of industry asks

The table below summarises the primary principles and objectives that the UK-based FRPS industry would like to see taken forward by UK government and regulators with US counterparts. If these asks are achieved, businesses and consumers in both markets will be able to realise many of the benefits of a transatlantic digital market, from enhanced consumer choice to more jobs and investment.

Although this report focuses on the UK-US trading relationship, many of the principles and objectives will also apply to negotiation meetings with other WTO members; such as Australia, Canada, New Zealand and Japan.

Summary of trade principles and objectives

PRINCIPLE	OBJECTIVE
• Encourage the free-flow of data in FRPS.	• Agreement that UK and US regulators will cooperate and share relevant data where needed for the other party's financial or regulatory investigations. Also make provision for the necessary sharing of data within the private sector.
• Address a market access barriers that impact FRPS firms operating between the UK and US.	• Enhanced commitment between the UK and US federal regulatory authorities to share certain financial information including foreign exchange reserves in the interest of greater transparency e.g. to help both parties determine benchmarking standards post-LIBOR.
• Identify ways to obtain fairer and more open conditions of trade in FRPS between the UK and US.	• A commitment to permit a financial or professional services firm that is regulated in either jurisdiction to transfer information (that is relevant to their licenced activities) into and out of that jurisdiction.
• Ensure both the UK and US maintain their ability to control and set their own domestic prudential requirements related to financial related and professional services.	• Introduce regulatory processes to allow for UK and US insurers and credit rating agencies to share information to allow for market development and the offering of more cross-border services.
• Remove any restrictions that require financial services or professional services firms to use or install local computing servers.	• Agree that cross-selling of financial services and professional services products will not apply to government procurement of financial or professional services.
• Mutual recognition that either party's domestic data protection laws will supersede any provisions requiring the free-flow of data.	• Establish a committee to review upcoming prudential regulations in each jurisdiction, at a high-level, in advance of them coming into effect to allow for more regulatory alignment.
• Tackle cross-border financial crime and anti-money laundering through the sharing of information to build profiles on those involved in fraud and monitor the market.	
• Work together in counteracting cyber terrorism and to engage in industrial practices to determine the ability of a potential hacker to access sensitive financial or professional services data.	

APPENDIX
EXAMPLES OF COUNTRIES WITH DATA LOCALISATION LAWS

Australia	
Relevant law	The Personally Controlled Electronic Health Records Act 2012 (PCEHR Act),[58] has now been superseded by the My Health Records Act 2012.[59]
Date law came into effect	The PCEHR Act contained provisions in respect of the disclosure to third parties and the archiving of cancelled records. Such provisions have now been amended by the My Health Records Act 2012. This is a compilation of the My Health Records Act 2012 and is the latest version, showing the text of the law as amended and in force on 11 December 2018 (compilation date).[60]
Comments	It has been stated that the PCEHR Act prohibited the transfer of personal health information outside of Australia[61]; although this will need to be considered in light of the new My Health Records Act 2012.

[58] Australian Government, 'Personally Controlled Electronic Health Records', (February 2012), available at: https://www.legislation.gov.au/Details/C2012A00063
[59] Australian Government, 'My Health Records Act 2012', (December 2018), availabe at: https://www.legislation.gov.au/Details/C2018C00509
[60] Ibid.
[61] The Columbia science and technology law review, 'The Emerging Trend of Data Localization', (March 2018), available at: http://stlr.org/2018/03/01/the-emerging-trend-of-data-localization/

Brunei Darussalam

Relevant law	There is no current comprehensive law on data protection, but the country has been guided by a Data Protection Policy since 2014 (Data Protection Policy; Policy).[62] The Policy covers personal data (in electronic or manual form) maintained by government agencies and educational institutions.
Date law came into effect	As already stated, our understanding is that the data protection laws of Brunei Darussalam are guided by its Data Protection Policy. This was last revised on 27 August 2015.[63]
Comments	The Data Protection Policy as referred to under section 18 (Principle XI – Trans-border Data Transfers) refers to the ability of Agencies to transfer 'Personal Data'[64] to another party (other than the organisation or the Individual) outside of Brunei Darussalam only if: • the Agency reasonably believes that the recipient of the data is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the data that are substantially similar to the data protection principles in this Policy • the Individual consents to the transfer; • the transfer is necessary for the performance of a contract between the Individual and the Agency, or for the implementation of pre-contractual measures taken in response to the data subject's request; • the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between the Agency and a third party • the Agency or Individual has taken reasonable steps to ensure that the data which it has transferred will not be held, used or disclosed by the recipient of the data inconsistently with the data protection principles in this policy.[65]

[62] E-Government National Centre, 'Data protection policy', (August 2015), available at: http://www.information.gov.bn/PublishingImages/SitePages/New%20Media%20and%20IT%20Unit/Data%20Protection%20Policy%20V.2.2.pdf
[63] Ibid.
[64] Ibid., 2.1.22. Personal Data - data, whether true or not, about an individual who can be identified (a) from the data; or (b) from the data and other information which is in the possession of, or is likely to come into the possession of, the Agencies.
[65] Ibid., 18. Trans-border Data Transfers

Canada

Relevant law	The Personal Information Protection and Electronic Documents Act (PIPEDA) protects consumer data across Canada.[66] Canadian provinces can impose additional regulations that sectors must follow, such as: • The British Columbia's Personal Information Protection Act [SBC 2003] Chapter 63 (PIPA) • The Nova Scotia's Personal Health Information Act (PHIA).
Date law came into effect	The PIPEDA (the complete version) received Royal Assent on 13 April 2000, and was last amended on 23 June 2015.[67] British Columbia's PIPA came into effect in January 2004.[68] The Nova Scotia PHIA came into force on 1 June 2013. The PHIA governs the collection, use, disclosure, retention, disposal and destruction of personal health information. It gives citizens a right to file a 'Request for Review' of decisions made by health custodians to the staff of the Office of the Information and Privacy Commissioner for Nova Scotia (NS OIPC).[69]
Comments	In Canada, it has been stated that federal law contains no data localisation requirements. However, provincial laws in British Columbia and Nova Scotia require that personal information created by public institutions (for example, government agencies, schools, hospitals and utilities) must be stored on servers located in Canada. These laws also require that the data is to be accessed from within Canada.

[66] The PIPEDA is the federal privacy law for private-sector organisations. It sets out the ground rules for how businesses must handle personal information in the course of commercial activity - Office of the Privacy Commissioner of Canada, 'The Personal Information Protection and Electronic Documents Act (PIPEDA)', (May 2019), available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[67] Office of the Privacy Commissioner of Canada, 'PIPEDA legislation and related regulations', (January 2018), available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

[68] Office of the Information and Privacy Commissioner for British Columbia, 'Legislation', (august 2019), available at: https://www.oipc.bc.ca/about/legislation/

[69] Office of the Information and Privacy Commissioner for Nova Scotia, 'About', (August 2019), available at: https://oipc.novascotia.ca/about-the-review-office

China	
Relevant law	China's Cybersecurity Law (CSL).
Date law came into effect	China's CSL was passed on 7 November 2016 and came into force 1 June 2017. It was stated that the data localisation provision of the CSL came into effect on 31 December 2018.[70]
Comments	Article 24 and Article 61 require that all telecommunication service providers and instant messaging services request real-name registration from their users and pass the collected data to the government for law enforcement purposes. The regulation governing cross-border data transfer was delayed and was implemented at the end of 2018. Article 37 of the CSL also requires 'critical information infrastructure' operators to store within mainland China all personal information and important data gathered or produced within the mainland territory. The definition of 'critical information infrastructure' is introduced in Article 31 to include (but is not limited to): "public communication and information services, energy, transportation, water resources, finance, public services [and] e-governance". The law further requires a security assessment of the locally stored data if a cross-border data transfer is necessary (Article 37). Data localisation requirements have also been included in various Chinese internet-related legislation. For example and as early as in 2011, China's central bank made a guideline that provides 'financial information collected in China's territory' to be 'stored, processed and analysed' within China's border.[71]

[70] The Law Reviews, 'The Privacy, Data Protection and Cybersecurity Law Review - Edition 5', (October 2018), available at: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175626/china

[71] University of Washington, 'Chinese Data Localization Law: Comprehensive but Ambiguous', (February 2018), available at: https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/

Germany

Relevant law	The German Federal Data Protection Act.[72]
Date law came into effect	25 May 2018.[73]
Comments	Although Germany does have federal legislation in place on data, data requirements vary by state. For example, the German state of Brandenburg requires that data on residents can only be stored on cloud computing services located in the state. Germany's Commercial Code[74] also requires companies to store accounting data and documents locally. And Germany's tax code requires all persons and companies liable for German taxes to keep accounting records in Germany (with some exceptions for multinational companies).[75]

India

Relevant law	The Reserve Bank of India (RBI) issued a directive under section 10(2) of the Payments and Settlement Systems Act 2007.
Date law came into effect	India's Payments and Settlement Systems Act 2007 is dated (draft) 20 December 2007.[76]
Comments	In April 2018, the RBI issued a new rule for payment systems providers operating in the country. Under the rule, all user data collected within the borders of the country needed to be localised within six months. The RBI said it was motivated by the need to have; 'unfettered supervisory accesses' to such data, given the fast-growing and increasingly technology dependent payments ecosystem in India. This new data protection rule is part of a larger set of multi-sectoral data protection and privacy measures being considered in India. Such provisions are set out in the draft Personal Data Protection (PDP) Bill in July 2018. The PDP Bill is currently in draft form.[77]

[72] The International Association of Privacy Professionals, 'Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680', (June 2017), available at: https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf

[73] Ibid., 61 - Article 8. Entry into force and expiry - (1) This Act shall enter into force on 25 May 2018, subject to subsection 2. The Federal Data Protection Act in the version published on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 7 of this Act shall expire at the same time. (2) Article 7 shall enter into force on the day following its promulgation

[74] Das Bundesministerium der Justiz und für Verbraucherschutz, 'Handelsgesetzbuch', (August 2019), available at: ('http://www.gesetze-im-internet.de/hgb/index.html

[75] United States International Trade Commission, 'Global Digital Trade 1', (August 2017), available at: https://www.usitc.gov/publications/332/pub4716.pdf

[76] Atlantic Council, 'India's Data Localization Efforts Could Do More Harm Than Good', (February 2019), available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/india-s-data-localization-efforts-could-do-more-harm-than-good

[77] News18, 'Data Privacy Day: What to Expect When The Personal Data Protection Bill Gets Tabled This Summer', (January 2019), available at: https://www.news18.com/news/tech/data-privacy-day-what-to-expect-when-the-personal-data-protection-bill-gets-tabled-this-summer-2016613.html

Iran

Relevant law	Draft data protection bill.
Date law came into effect	The Iranian Minister of Communications and Information Technology, Mohammad Javad Azari Jahromi, announced on 26 July 2018, that the government had prepared a draft data protection bill.[78]
Comments	Iran does not have a personal data-protection act per se, but it has been moving towards developing its own national intranet—the Halal Internet—to separate itself from the rest of the internet. This also includes a move toward greater data localisation.[79] Iran's government operates an extensive online censorship regime. During political protests in 2009, Iran blocked Facebook, Twitter and YouTube. In 2015, Iran launched its own search engines which only show approved websites. In August 2016, Iran set up its first government-paid cloud data centre. In May 2016, Iran ordered foreign messaging apps, such as WhatsApp to store data from Iranian users locally.[80]

Indonesia

Relevant law	The Government Regulation No. 82 of 2012 on Implementation of Electronic System and Transaction (Regulation No. 82).
Date law came into effect	The Government Regulation No. 82 of 2012 on the Electronic System and Transactions was issued on 12 October 2012 to implement certain aspects of Law No. 11 of 2008 on Electronic Information and Transactions.[81]
Comments	There has been some uncertainty in respect of the data localisation requirements in Indonesia as referred to under Regulation No. 82. Under Regulation No. 82, an electronic system operator that provides a public service must place its data centre and disaster recovery centre in Indonesia. However, Regulation No. 82 does not define what a 'public service' means, which makes it difficult for electronic system operators in Indonesia to determine whether or not they are subject to the requirement.[82]

[78] Data Guidance, 'Iran: Government drafts first data protection bill', (August 2018), available at: https://www.dataguidance.com/iran-drafts-data-protection-law/

[79] Information technology and innovation foundation, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?', (May 2017), available at: https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

[80] The Financial Conduct Authority, 'Global AML and Financial Crime TechSprint', (March 2019), available at: https://www.fca.org.uk/events/techsprints/aml-financial-crime-international-techsprint

[81] Lexology, 'Indonesia - changes to data localization provisions for electronic system operators', (August 2019), available at: https://www.lexology.com/library/detail.aspx?g=a3b371a0-1b95-4ebc-86a1-2cbcda491eda

[82] Lexology, 'Indonesia proposes amendments to its data localisation requirement', (December 2018), available at: https://www.lexology.com/library/detail.aspx?g=a116020b-cee3-433f-b62b-a5e988477d8e

Malaysia

Relevant law	Personal Data Protection Act 2010 (PDPA).
Date law came into effect	The PDPA came into force on 15 November 2013.[83]
Comments	Section 129(1) of the PDPA states that a company may only transfer personal data out of Malaysia if the country is specified by the Minister of Communications and Multimedia Malaysia and this is then published in the Gazette. The Commissioner had issued a Public Consultation Paper entitled; 'Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 (the Proposed Order 2017),[84] which seeks feedback from the public on the Commissioner's draft whitelist of countries to which the personal data originating in Malaysia may be freely transferred without having to rely on exemptions provided by Section 129(3) of the PDPA.[85]

Nigeria

Relevant law	Nigeria's National Information Technology Development Agency (NITDA) issued the Nigeria Data Protection Regulation 2019.[86]
Date law came into effect	25 January 2019.
Comments	It has been stated that in respect of data transfers, transfers of personal data outside of Nigeria may take place only if certain specified criteria are met.

[83] PwC, 'Personal Data Protection Act 2010 (PDPA)', (November 2013), available at: https://www.pwc.com/my/en/services/assurance/pdpa.html
[84] The Law Reviews, 'Malaysia', (October 2018), available at: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175635/malaysia
[85] Taylor Wessing, 'Data protection in Malaysia', (May 2014), available at: https://globaldatahub.taylorwessing.com/article/data-protection-in-malaysia
[86] The National Information Technology Development Agency, 'Nigeria data protection regulation', (January 2019), available at: https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf

Philippines

Relevant law	The National Privacy Commission (NPC) is the regulatory agency tasked to administer the Philippines' Data Privacy Act of 2012 (DPA). In respect of data privacy-related regulations of the Philippine Insurance Code and regulations issued by the Philippine Insurance Commission (IC) the same is administered by the IC.[87]
Date law came into effect	The Data Privacy Act of 2012 is referred to as beginning and held in Metro Manila on 25 July 2011.[88] The DPA and its implementing rules and regulations (DPA IRR) is stated to have taken effect on 9 September 2016.[89]
Comments	The Philippines has strict consent requirements and regulatory approvals for overseas data transfers, which has been referred to as forcing data localisation within the national country.[90]

Russia

Relevant law	Federal Law No. 242-FZ.
Date law came into effect	Russia's data localisation law was adopted as a set of amendments to Russia's On Personal Data Law in July 2014 and was intended to come into force on 1 September 2016. However, in late 2014, Russian President Vladimir Putin signed a law changing the data localisation law's effective date from 1 September 2016 to 1 September 2015.[91]
Comments	The law requires 'operators' to collect, store and process Russian citizens' personal data using databases located within Russia. Operators must also must inform Russia's Roskomnadzor (the state body that oversees telecommunications, information technology, and mass communication) of the location of the servers where Russians' personal data is stored.[92]

[87] Baker McKenzie, 'Asia Pacific Guide to Data Protection and Cybersecurity for Insurers', (September 2017), available at: https://apinsurance.bakermckenzie.com/-/media/asia-pacific-regulatory-landscape-and-issues-in-ba/files/baker-mckenzie-asia-pacific-guide-to-data-protecti.pdf?la=en

[88] National Privacy Commission, 'Republic Act 10173 - Data Privacy Act of 2012', (https://www.privacy.gov.ph/data-privacy-act/

[89] Baker McKenzie, 'Asia Pacific Guide to Data Protection and Cybersecurity for Insurers', (September 2017), available at: https://apinsurance.bakermckenzie.com/-/media/asia-pacific-regulatory-landscape-and-issues-in-ba/files/baker-mckenzie-asia-pacific-guide-to-data-protecti.pdf?la=en

[90] The Public Sphere, 'Data localization laws in a digital world', (February 2016), http://publicspherejournal.com/wp-content/uploads/2016/02/06.data_protection.pdf

[91] Proskauer, 'A Primer on Russia's New Data Localization Law', (August 2015), available at: https://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/

[92] WILmap, 'Federal Law No. 242-FZ.', (July 2014), available at: https://wilmap.law.stanford.edu/entries/federal-law-no-242-fz

South Korea	
Relevant law	Amendment made to the Act on the Promotion of IT Network USE and Information Protection (Network Act).
Date law came into effect	In effect from 19 March 2019.
Comments	Amendments require digital communications providers who collect South Korean citizens' data and do not have a physical presence in the country to install a domestic representative to oversee data protection issues.

Turkey	
Relevant law	One example: Law on Payment and Security Reconciliation Systems, Payment Services and Electronic Money Organisations.[93]
Date law came into effect	The date of acceptance of this law is referred to as 20 June 2013.
Comments	There are sector-specific laws requiring data controllers to store data in Turkey for at least 10 years.

Vietnam	
Relevant law	The Law on Cybersecurity.
Date law came into effect	On 12 June 2018, the Vietnamese National Assembly passed the Law on Cybersecurity (Cybersecurity Law), which took effect on 1 January 2019.
Comments	Law requires companies that collect, analyse or process personal data from Vietnamese customers to have a physical office and store users' data in Vietnam.

[93] Türkiye Cumhuriyet Merkez Bankası, 'Law on payment and securities settlement systems, payment services and electronic money institutions', (June 2013), available at: http://www.tcmb.gov.tr/wps/wcm/connect/de4fb4cc-19c4-47fe-a9cb-9ef0397a8923/1.+LAW.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-de4fb4cc-19c4-47fe-a9cb-9ef0397a8923-m3fw3yl

For further information about this report contact:

Gary Campkin,
Managing Director, External Relationships and Strategic Issues, TheCityUK
gary.campkin@thecityuk.com

Scott Devine,
Head, Africa, the Middle East & Legal Services; Head of North America (maternity cover), TheCityUK
scott.devine@thecityuk.com
+44 (0)20 3696 0109

TheCityUK

TheCityUK, Salisbury House, Finsbury Circus, London EC2M 5QQ
www.thecityuk.com