

# The UK Data Economy After Brexit: Enchanted Garden or Frozen Tundra?

Lucie Burgess  
Naima Camara  
Andreas Demetriou  
Brian MacAulay

October 2017

# Contents

- 1 **Executive summary**
- 5 **About Digital Catapult**
- 6 **About the authors**
- 7 **Introduction**
- 12 **Data markets, data trade and data flows**  
The UK in the context of the European and global data economy
- 20 **A tale of two countries**  
Data protection regulation in the UK and US
- 28 **Opportunities and risks for the UK data economy post-Brexit**  
Four scenarios
- 40 **Views from the roof**  
Insights from industry and policy makers
- 46 **Conclusions**  
Considerations for industry and policy makers
- 52 **Bibliography**

# Executive summary

## The UK Data Economy After Brexit: Enchanted Garden or Frozen Tundra?

The UK is currently on firm ground with a sizeable, competitive and growing data economy, worth approximately 2% of GDP in 2016. While the UK will leave the EU in a strong position from the perspective of the data economy, Brexit presents the UK data economy with both opportunities and downside risks to be mitigated. On the one hand, the opportunity to simplify data protection legislation while maintaining EU 'adequate' status may enable the UK to become a vital hub for data between the EU and the US. On the other hand, access to the EU Digital Single Market is uncertain and may bring both benefits and risks. The UK has the potential to bring the data economy to the fore during Brexit negotiations as a component of trade deals with major world economies. Whatever the future holds, data should be considered a vibrant and important part of the UK economy.

Personal data is central to every aspect of our digital lives such as social media, online banking, shopping, health and fitness and our work. The UK is a leader in the provision and use of data; recently the European Commission estimated the UK's share of the European data economy to be 20.4%<sup>1</sup> and its share of the European data market to be 22.4%, greater than its share of GDP at 17.3%. With the ever increasing amounts of data generated by new technologies, such as the Internet of Things, new issues have arisen in the tension between technological advancement and privacy.

On 23rd June 2016 the UK electorate voted to leave the European Union. Just prior to that, in May 2016, the European Parliament laid down in Europe's statute books the General Data Protection Regulation (GDPR) which the UK government has confirmed will become law in the UK in May 2018. At the time of publication of this report in October 2017, the UK Data Protection bill was in passage through the House of Lords. GDPR overhauls privacy legislation at a time when information systems and digital business are integral to daily life; it sets out new provisions for privacy-by-design, data portability, transparency, consent, and the imposition of heavy fines for non-compliance.

Digital Catapult set out to understand what impact these events might have on the market for data and the wider data economy. Given the centrality of data to the UK technology sector and its

changing position in Europe, what might the opportunities and benefits be? Where might there be challenges and risks, and what adjustments could be made to policy or regulation as a result? What could be learnt from the balance between business practice and privacy legislation in the United States, the world's largest data economy? How might Brexit provide an opportunity to re-position the UK in terms of data flows between the US and Europe and what conditions might be necessary to achieve this?

In order to answer these questions, Digital Catapult conducted primary and secondary research to understand the landscape of privacy legislation and regulation in the context of the UK data market and the wider data economy. It posed four extreme scenarios to help it conduct a 'thought experiment', based on the degree of access to the EU Digital Single Market and the ability for UK data businesses to reformulate and influence data protection law, using the GDPR as a baseline. Digital Catapult interviewed a number of data-intensive companies, policy-makers and academics including representatives from the Information Commissioner's Office (ICO), the Department for Culture, Media and Sport (DCMS), the Department for International Trade (DIT), UKCloud, Meeco, Swiss Re, Ocado, Founders4Schools, CrowdEmotion, Squire Patton Boggs, the Royal Society and senior academics from Queen Mary University of London. Digital Catapult is grateful for the expertise and insight of all those who contributed their perspectives.

<sup>1</sup> IDC/ European Commission, The European Data Market Final Report: Study Dataset, <http://www.datalandscape.eu/study-reports>. 2016 total data economy value (total impacts) in the UK as a percentage of total EU28.

Digital Catapult's report makes a series of suggestions for policy makers and industry and raises questions for further inquiry which have so far not been considered widely. Digital Catapult believes these considerations could positively impact the growth of the UK data market post-Brexit, setting the right conditions in place for the UK data market to reach the €26.2 billion high-growth scenario forecast by the European Commission by 2020 or €166.8 billion for the overall UK data economy. However, there are also substantial equivalent risks to the data economy from leaving the European Union and not implementing these suggestions.

The four extreme scenarios demonstrate the benefits and risks of access to the Digital Single Market, particularly the market for data (with impacts on the wider data-driven economy), and approach to data protection law. The scenarios are:

- 1. Frozen Data Tundra:** UK without access to the Digital Single Market and imposition of GDPR with less capacity to influence regulation. This scenario represents the possibility of the frozen state of data trade and data innovation.
- 2. Wild Data Allotment:** UK without access to the Digital Single Market, but businesses are able to influence regulation; representing less access to markets compared to more regulatory influence enjoyed by businesses.
- 3. Stagnant Data Island:** UK with full access to the Digital Single Market, but limited business ability to influence the regulatory regime. This scenario demonstrates the trade-off incurred to gain access to the Digital Single Market to the detriment of business' ability to influence regulatory policy.
- 4. Enchanted Data Garden:** UK with full access to the Digital Single Market, while businesses simultaneously influence the data legislative agenda; references the abundant possibilities of data innovation and blossoming of UK data-intensive business, if the UK obtains full access to the Digital Single Market with businesses simultaneously being able to influence data protection legislation.

This report compares and contrasts the UK and US privacy regimes; the US three-tier approach, set by precedent at state and sector level, is reasonably agile, but lacks clarity and many commentators perceive leans towards businesses over individuals' rights. The UK approach has a reputation for being firm but fair and achieves a balance in comparison to European counterparts which are perceived as taking a more stringent approach. It is worth noting that the implementation of GDPR at the same time as Brexit may leave the UK in a position where it is subject to European data protection regulation but comparatively unable to influence it, as it will not be a member of the EU Data Protection Board. At the time of publishing this report, the UK's Data Protection Bill was in passage through the House of Lords. The UK will in future have the freedom to implement further changes, the key question being whether its own domestic data protection law is considered 'adequate' by the EU.

**This report makes five suggestions for policy makers and researchers to take forward and for UK businesses to be aware of in their Brexit planning:**

#### **Consideration 1**

**Negotiators should ensure that data flows, data markets and the wider data economy are taken into consideration in any UK-EU trade deal.**

Traditionally, trade deals focused on physical goods and commodities and less so on intangible assets such as data. In fact there is an absence of data-related provisions in international trade agreements, and this report suggests that this should be an area for policy-makers and governments to consider as global economies become increasingly knowledge-based.

#### **Consideration 2**

**Explore the conditions around an attractive UK-US trade deal which positions the UK as a data hub.**

Despite disparate regulatory regimes, Brexit provides an opportunity for the UK and US to strike a bilateral trade deal which should include data as a consideration. An improved UK-US trade deal could give the UK at a more advantageous position in transatlantic trade than its European counterparts. It also strengthens the possibility of the UK acting as a data 'hub' between the US and Europe. However, sectoral and geographic interests will influence parliament and hence they will have to be appeased, meaning that making a "quick" and "good" trade deal with a comparably good data-related aspect, may be beyond the intentions and altruism of the US and UK governments.

### Consideration 3

#### Simplify UK data privacy regulation compared to GDPR.

Brexit provides an opportunity in the context of data privacy to simplify the UK's regulatory regime, in order to be considered adequate by the EU, while still ensuring that its privacy regime supports innovation in the growing data economy. At its most beneficial, Brexit provides the opportunity for the UK to implement a new form of post-GDPR legislation inspired by the US model that it is deemed 'adequate'. Although the UK may not form part of the EU single market per se, it must strive to obtain access to the as yet nascent Digital Single Market by achieving adequacy status for data transfers. In doing so, the UK will have the opportunity to act as a 'hub' between Europe and the US. However, there is the risk that the UK could find itself with limited access to the Digital Single Market, it deemed inadequate by the European Commission and subject to GDPR with UK businesses holding little influence over the regime.

### Consideration 4

#### Put in place measures to avoid localisation of data businesses to the UK.

Localisation of data businesses to the UK is a significant risk for the UK post-Brexit. Localisation refers to the requirement that a firm maintains its data, and hence related facilities and personnel in the market, country and regulatory space where it operates. The risk of localisation to the UK data economy could be substantial. Several interviewees raised concerns about what the localisation arrangements would be post-Brexit, which highlights the extent to which more guidance is needed from policy makers. Essentially Brexit negotiators should ensure that UK companies do not have to segregate data between the UK and the EU.

### Consideration 5

#### Use industry-wide voluntary data privacy standards as an alternative form of regulation.

The use of industry-wide or sector specific data privacy standards can offer an alternative or complement to regulation through legislation. Sector-specific certification and standards schemes offer the possibility of compliance with the spirit of the legislation with greater sectoral reliance of flexibility. The research highlighted the continued disparity between the speed of technological advancements and the creation, implementation and enforcement of regulatory reform. Therefore, standardisation should not be not as a compromise for robust data protection policy, but to supplement GDPR and attempt to bridge the gap between the speed of advancements by data-intensive businesses and privacy policy.

#### This report explores the UK and EU data relationship post-Brexit and notes three risks:

- Firstly, addressing data transfers might not be considered a salient enough topic to be included in the negotiations at all, either due to the need for simplicity or due to complexity of data transfer issues.
- Secondly, it might not be in the interests for UK negotiators to consider data in the Brexit trade deal. It might be the case, that at least for the next two years, the data sharing relationship of the EU and the US changes and this has a direct impact on the UK's ideal negotiating position on data in the EU trade agreement.
- Thirdly, it is not clear whether negotiations on data trade should they happen will result in "less policy flexibility for more market access" and vice-versa.

Although the probability of each of the above points is arguably individually low, their summative likelihood is potentially significant. That is, there is a fair chance that Brexit negotiators will marginalise the issue of data transfers and/or avoid including it in the initial negotiations and/or involve it in a cross-sectoral trade-off. Given the importance of the data economy, this is both a risk and a missed opportunity.

## Conclusion

The UK's future position outside the EU places the UK in a unique position. Clarity on the level of access to the Digital Single Market and the amount of freedom for businesses to inform data privacy regulation are essential to understanding the data economy post-Brexit. This report draws five considerations for further enquiry, research and policy intervention to counteract the risks and take advantage of any post-Brexit opportunities. Exploration of these five suggestions could bring the UK as close as possible to the scenario of 'enchanted data garden', which would allow UK businesses full access to the Digital Single Market and enable businesses to inform the direction of privacy regulation in the coming years, positioning the UK as a data hub between the US and Europe. This report suggests this could bolster the nation's economic potential with respect to data markets and the wider data economy and in doing so allow the UK to maintain its position as a premier destination for data in the post-Brexit world.

**Drawing on the published IDC scenario projections to 2020, the 'challenge' and 'high growth' scenarios, this report has sought to estimate the potential economic benefits of our proposed data privacy regulation and Digital Single Market access scenarios.**

- Starting from a position within Frozen Data Tundra, if we enable increased flexibility in data regulation but assume restrictions on market access the projected potential impacts are between €17 billion and €25 billion.
- Again starting from Frozen Data Tundra, if we apply a restriction to the flexibility in data regulation but assume complete access to the EU Digital Single Market the projected potential impacts are between €11 billion and €42 billion.
- Combining increased data flexibility with complete access to the EU Digital Single Market i.e. entering the Enchanted Data Garden, we estimate a projected potential impact of between €28 billion and €67 billion.

*Digital Catapult would like to thank the businesses, organisations and individuals who contributed their perspectives and expertise to this report.*

## About Digital Catapult

Digital Catapult is a technology innovation centre that unlocks digital growth in the UK economy. It works with companies of all sizes to transform their businesses by accelerating the practical application of digital innovation. We bridge the gap between research and industry, finding the right technologies to solve problems, increase productivity and open up new markets faster.

Digital Catapult connects experts with established enterprises, start-up and scale-up businesses, and researchers to discover new ways of solving big technological challenges in the digital manufacturing and creative industries.

It provides experimental and testing facilities and access to experts so that new services and applications can be trialled to market faster and we do this across the UK via our five innovation centres. This breaks down barriers to technology adoption for start-ups and small businesses, de-risks innovation for enterprises and uncovers new commercial applications for digital technology in the fields of immersive, connectivity, data and artificial intelligence.

## About the authors

### **Lucie Burgess**

Head of Personal Data and Trust at Digital Catapult; Senior Research Fellow at Hertford College, University of Oxford.

### **Naima Camara**

Policy and Research Coordinator at Digital Catapult.

### **Andreas Demetriou**

Researcher at Digital Catapult at the time of writing.

### **Brian MacAulay**

Lead Economist at Digital Catapult.



# Introduction

Over the last century, knowledge has become central to economic development. A wealth of technologies have emerged in the UK and abroad. The increasing digitisation of our personal lives and economic activities have resulted in the prolific generation of various kinds of personal and non-personal digital data. According to the European Commission (EC), the 'value of the data economy will increase to €643 billion by 2020, representing 3.17% of the overall European GDP.'<sup>2</sup> Similarly, according to the UK government's Digital Strategy, 'analysis predicts that data will benefit the UK economy by up to £241 billion between 2015 and 2020.'<sup>3</sup>

In fact, the UK is a leading country in the utilisation of data; it ranks first among EU countries in terms of data openness and second worldwide, with a score of 76%.<sup>4</sup> Similarly, its share of the European Data Market is at 22.4%, 3.3% higher than the UK 17.4% share of the EU GDP.<sup>5</sup> In addition, the International Data Corporation (IDC) predicts in the European Data Market Report, that even taking Brexit into consideration, the UK will remain a dominant force in terms of data revenue in 2020 along with other large EU economies.<sup>6</sup> This level of growth is due to the ever-increasing amounts of data generated by machines based on emerging technologies.<sup>7</sup> However, new issues have arisen regarding the protection of the rights of UK citizens, as both can be jeopardised if data, and personal data in particular, are stored, transferred or processed irresponsibly.<sup>8</sup>

Europe has long been attempting to reconcile this ever-increasing tug of war between technological advancement and personal privacy. In fact, the UK's data protection authority (DPA), the Information Commissioner's Office (ICO), along with other regulatory authorities, have spearheaded efforts to form and introduce the (EU) 2016/679 General Data Protection Regulation (GDPR), due to be enforced in May 2018 and to repeal Directive 95/46/ EC.<sup>9</sup> GDPR will overhaul Europe's cornerstone data protection legislation<sup>10</sup> at a time when information systems and digital technology underpin human life. Several key concepts are embodied in GDPR: right to erasure, data portability, data breach notification and accountability.

This regulation will come into force in all EU Member States on 25th May 2018 when the UK remains a member of the EU. However, the UK will leave the EU shortly afterwards, which places us in a unique position to re-evaluate future data regulatory framework. Although there is much uncertainty surrounding Brexit, the Prime Minister's speech on January 17th 2017, the release of the United Kingdom's Exit from and New Partnership with the European Union<sup>11</sup> and the triggering of Article 50 have provided the foundation for several assumptions.

---

2 "Building the European Data Economy," 10 January 2017, [http://europa.eu/rapid/press-release\\_MEMO-17-6\\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-6_en.htm).

3 UK Digital Strategy", 1 March 2017, <https://www.gov.uk/government/publications/uk-digital-strategy>.

4 Global Open Data Index, "Place Overview," 2016. <https://index.okfn.org/place/>

5 IMF 2016; Cattaneo, G. "The European Data Market." IDC presentation given at the NESSI summit in Brussels on 27 (2014).

6 IDC, "European Data Market." <http://www.datalandscape.eu/study-reports>, 107.

7 "Building the European Data Economy," January 10, 2017. [http://europa.eu/rapid/press-release\\_MEMO-17-6\\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-6_en.htm).

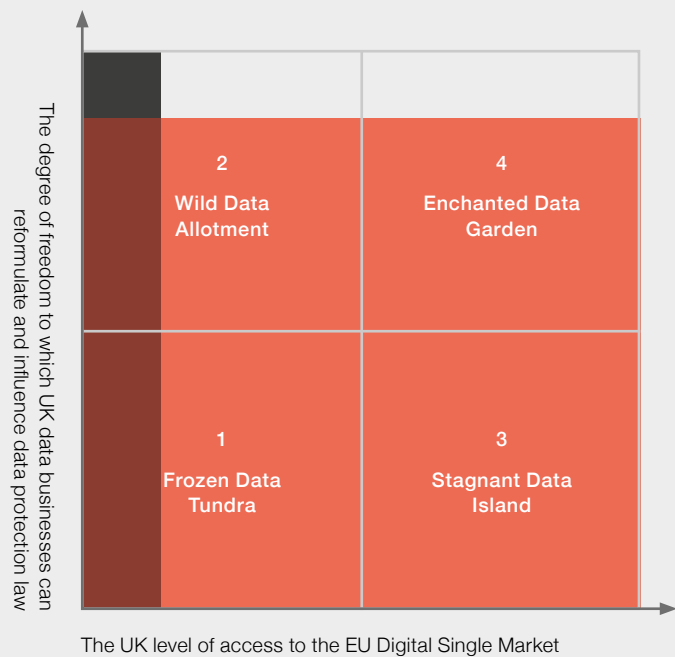
8 CMA, "The Commercial Use of Consumer Data", 2015. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/435817/The\\_commercial\\_use\\_of\\_consumer\\_data.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf)

9 95/ 46/ EC (General Data Protection Regulation)." Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/ 46/ EC (gen. n.p. [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf).

10 Bird & Bird All Rights Reserved, Guide to the General Data Protection Regulation, (London: Bird and Bird LLP, 2016), 2.

11 UK Government, "The United Kingdom's exit from and new partnership with the European Union". [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/589191/The\\_United\\_Kingdoms\\_exit\\_from\\_and\\_partnership\\_with\\_the\\_EU\\_Web.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589191/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf).

Figure 1:  
Four extreme scenarios produced by Digital  
Catapult in relation to market access and data  
privacy regulation.



Source: Digital Catapult Analysis

### Assumptions:

- The UK's level of access to the Digital Single Market is uncertain as a result of Brexit.
- GDPR will be implemented in the UK in May 2018 in some form.

These assumptions have led Digital Catapult to explore two variables:

- The UK's level of access to the EU Digital Single Market.
- The level of freedom for UK data businesses to influence and reformulate data privacy law in comparison to the EU GDPR.

These assumptions have provided a springboard for the exploration of four extreme scenarios in relation to the UK personal data market:

1. **Frozen Data Tundra**
2. **Wild Data Allotment**
3. **Stagnant Data Island**
4. **Enchanted Data Garden**

Evidently it is very difficult to determine with complete certainty at this stage what the UK's data protection regulation will look like post-Brexit, the extent to which the Digital Single Market will be achieved or the UK's access to it. In posing these four extreme scenarios Digital Catapult aimed to provoke debate and discussion for businesses and policy makers. Digital Catapult began by conducting a thorough literature review and desk-based research, then interviewed data business leaders, academics and policymakers in relation to the scenarios posed and their individual perspectives on the data economy.

The report aims to provide clarity by exploring the opportunities and risks that may arise for UK data-businesses given the uncertainty surrounding the post-Brexit personal data regulatory landscape, with a particular focus on personal data. In doing so, the report is divided into five chapters, as follows:

### **Data markets, data trade and data flows: the UK in the context of the European and global data economy**

Sets the UK data economy in context, analysing the scale and scope of data markets, data-trade, international data flows and the extent to which data is a component in Brexit negotiations. This first chapter contextualises the EU regulatory landscape for personal data as it relates to the UK.

### **A tale of two countries: data protection regulation in the UK and US**

Compares and contrasts the US and UK by analysing their respective data economies, approaches to privacy legislation and enforcement. It also discusses the possibility and impact of a UK-US trade deal post-Brexit.

### **Opportunities and risks for the UK data economy post-Brexit: four scenarios**

Analyses our extreme scenarios in more detail and outlines the opportunities and risks for the post-Brexit regulatory regime in relation to personal data. The report also discusses in more depth the possibility of a US-UK trade deal and the main considerations for the impending EU-UK trade deal.

### **Views from the roof: insights from industry and policy makers**

Presents the results of a series of expert interviews, conducted with firms, policy-makers and academics, with the explicit aim of understanding the strengths, weaknesses, opportunities and threats surrounding the uncertainties borne out of Brexit and future data protection legislation.

### **Conclusions: considerations for industry and policy-makers**

Uses evidence and arguments set out in previous chapters to present the areas and issues, which have been identified as most salient for the data privacy regulatory regime and EU market access post-Brexit. The report sets out five suggestions for industry and policy-makers to consider further.



# Data markets, data trade and data flows



The UK in the context of the  
European and global data economy

This chapter provides insights into the UK, EU and global data economies, the respective data markets and trade in data. Interestingly, there is an absence of data-related provisions in international trade agreements and Digital Catapult suggests this should be an area for policy-makers and governments to consider as global economies become increasingly knowledge-based.

## Types of data and its importance

In the most general sense, data can be described as an intangible quasi public good, as it is non-material, can be both excludable and non-excludable and is partially rivalrous (in that use of a data set by one user does often not diminish another user's ability to access and use the same data). Such generalisations however, are not particular enough in terms of helping us to understand the different forms that data can be found in, as an economic good.

### Commodity data

One such form is that of data as a "commodity". In some markets, such as mobile application development, or market-research and market-intelligence services, data takes the form of something to be generated or collected and sold onwards to potential buyers. In this case most of the value of these data lies in the complexity or difficulty of their collection process or their uniqueness and novelty. That is, the buyers of these data are looking to purchase information that is intended for further usage and are willing to pay a certain price, as collecting these data themselves would not be a good use of their resources, or would be beyond their technical or material capabilities.

### Common good data

A second form is that of data as "common good" (or "public good" as is the more general use of the term); these can be best described as "open data markets". Easy access to and interoperability of data is considered desirable, if not essential, for open data markets to operate at their maximum efficiency and potential. Examples may include the following: i) certain types of health services, where it is ideal for healthcare providers to have access to accurate and detailed medical records, both for personal healthcare as well as medical research purposes, and for patients to be able to switch from one provider to another for quality of service, financial or other reasons, knowing that their records are fully transferable; ii) policy research, where governmental, non-profit and other entities are often able to produce better and more accurate results in an environment where data are freely exchanged and easily accessible; and iii) 'Big Data' analytics services, which tend to generate more accurate and novel insights (and hence more value) through an environment where data-openness is sufficient for the creation of large data pools.

### 'Trade secret' data

In other markets, such as retail, data is more similar to a "trade secret" or intellectual property; carefully protected by the entity that is generating or collecting the data, and viewed as a competitiveness-enhancing asset that is not to be shared. Here, value comes primarily from improvements that the owner of the data can make to its product or service through the use of these data, and the degree to which these improvements help the owner to keep up with or even surpass its competition. Note that data as 'fact' does not attract intellectual property rights per se, although in Europe the arrangement of data in a database may attract *sui generis* database rights.

## The UK a leading data economy in Europe and the world

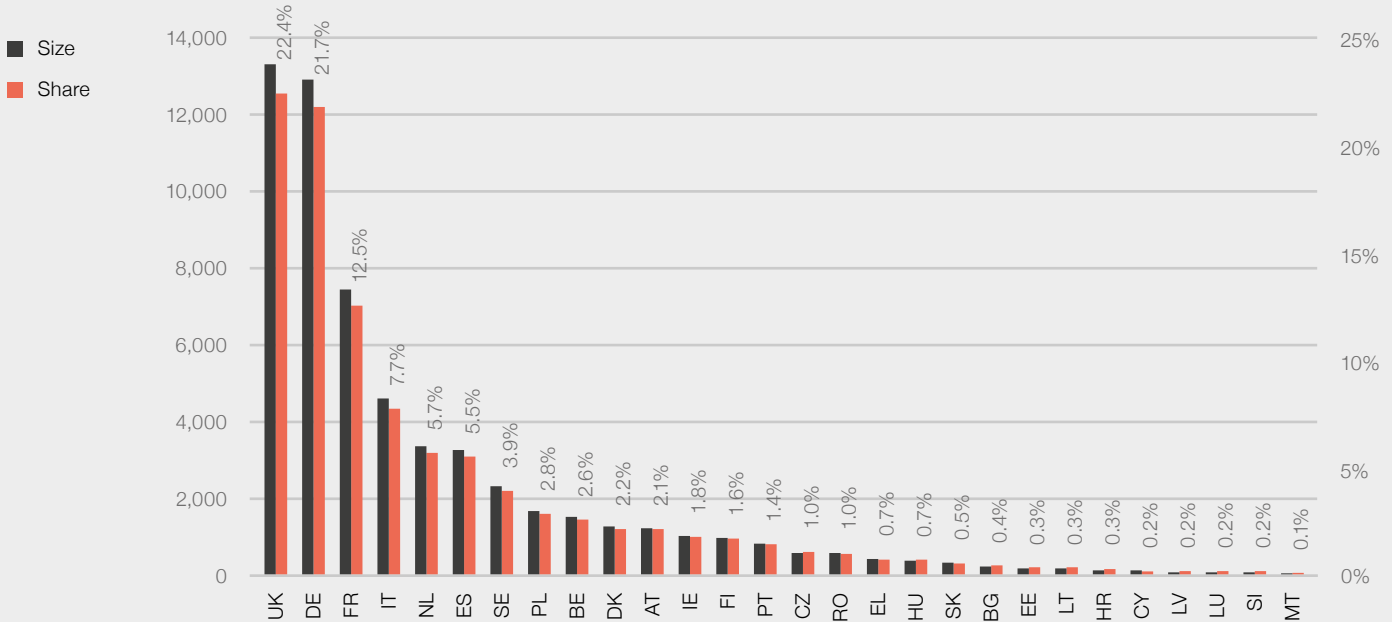
As is the case with novel technological changes, a precise methodology for measuring and understanding the impact of the increasing use of data, both in terms of quantifiable value and potential applications is lacking. Nevertheless, through this research, Digital Catapult has managed to gather and analyse a significant amount of empirical and theoretical information regarding the state of the UK data economy. For the purpose of this report, the data economy refers to the sum of all economic activities involving the collection, generation, processing, transfer and analysis of data, as well as the impact of these activities (including direct, indirect and induced impact). The data market relates to the contributions of IT software and hardware, including indirect IT services associated with the data market

THE UK DATA ECONOMY  
ACCOUNTED FOR AROUND

2%

OF UK GDP IN 2016

Figure 2:  
Data Market Value (£M) and Share of Data Market Value (%) by Member State, 2016.



Source: European Data Market Monitoring Tool, IDC 2016

In 2016, the UK data economy accounted for over 2% of the UK GDP with an estimated value of €61.3 billion. This places the UK data economy as the second largest in the EU, with Germany first at €77 billion, and fifth largest data economy worldwide, with the US the largest at €104 billion. In the case of the US, this estimate relates only to direct and backward direct impacts. Our analysis indicates these represent about 20% of the overall digital economy, so the overall US data economy is much higher. Applying this to Japan, where these elements are estimated by IDC to be €22.2 billion, their digital economy could be nearly €100 billion. There are no data available regarding the value of the Chinese data economy but, given the sheer size of the Chinese economy, it seems safe to assume that its value lies somewhere between Japan and the US. In general, the UK stands on very firm ground given its ability to develop and maintain a sizeable, competitive and growing data economy. It is well supported by a variety of educational, governmental and economic institutions that allow data businesses to grow and innovate with relative ease.

The number of UK data suppliers is disproportionately larger than other large EU economies, albeit with a rather average growth rate. In 2015, there were an estimated 120,500 data companies in the UK, about 95,000 more than Germany (a distant second) and more than 47% of the whole of the EU, which is estimated to have about 254,850 data companies in total. Similarly, in terms of data revenue, the UK leads the way, along with Germany as a close second, but with growth rates only slightly better than average. In

addition, the UK has the largest share of ICT spending in the EU at 23.7%, forecasts predict that the UK is to maintain this leading position, even under scenarios where future data economy growth is hypothesised as challenging.

The UK also has a sizeable and active data market, which for the purposes of this report is defined as the aggregate value of the demand for data products or services in the economy (Figure 1). In 2016, the value of the UK data market was estimated to be €13.313 billion, marginally higher than Germany's €12.9 billion, with above average growth levels at 13.2%. Projections of the growth of the EU data market by 2020 place the UK first at €17.7 billion, with Germany being a close second at €16.4 billion (France is a more distant third at €9.1 billion, and Italy fourth at €6.3 billion). IDC (co-author of the EU data market study) estimates the UK share of the EU data market to be the largest at 22.4%. In terms of the share of data market investment on ICT, the UK performs slightly below EU average at 9%, compared to 9.5% in 2016.

It is worth noting that under the three possible growth scenarios tested by IDC, the UK exhibits greater deviation (outcome variation) than other big EU economies: the variation for the UK in growth scenarios is between 4.7% and maximum 18.4%, in IDC's "challenge" and "high growth" scenarios respectively, although in each of the different growth scenarios the UK is expected to maintain its position as the largest data market in Europe. However, in terms of

data market baseline growth projections, the UK is expected to only equal to the EU average, with an annual average growth rate of 7.2% for the 2016-2020 period suggesting other countries are gaining. Analysis indicates Sweden and the Netherlands will grow at a faster rate increasing their share of the EU market by 2020.

### **There is misalignment between the technical and legal frameworks governing data transfers**

There appears to be a significant gap of knowledge and understanding between how data transfers take place technically and the legal framework that governs them. Businesses are understandably rather reluctant to share details of their data management arrangements such as the layout and workings of their enterprise architecture, networking arrangements, digital computation and storage facilities and use of cloud services. This secrecy, combined with sheer structural complexity, rapid rate of technological change and variety of approaches to data management, result in a form of unproductive ambiguity in regulation. When creating a legal framework for the protection of privacy rights, regulators and policy-makers can be faced with major difficulties in balancing privacy issues with the support of business operations and encouragement of innovation.<sup>12</sup> In addition, the need for stakeholder involvement and consultation during the process of the development of new regulations, along with the need for the regulation to undergo a certain degree of scrutiny and modification by the different political institutions involved, adds another dimension of challenges to the development of regulation. In turn, firms tend to rely on two separate mechanisms for filling legal and regulatory gaps in their operations, the first mechanism is the use of industry certifications, which serve the purpose of signalling compliance with certain standards to both customers and regulators. Secondly, and most importantly, firms create relevant contractual arrangements in order to fill any legal and operational gaps in their data transfer activities, vis-à-vis their interactions with both customers and businesses

### **International data trade increases productivity, living standards and welfare**

The utilisation of international data flows has been empirically shown to deliver increased economic efficiency and productivity benefits, as well as improvements in standards of living and welfare.<sup>13</sup> In 2014 alone, international data flows generated \$2.8 trillion in economic value surpassing the value of global trade in goods.<sup>14</sup> This is not only indicative of the rapid expansion and growth of the technology industry; it also reflects the digitisation of the economy as a whole. Data from the International Monetary Fund (IMF), show that from 2008 to 2012 cross-border information flows were fastest growing component of US as well as EU trade.<sup>15</sup> In fact, a study by leading economist, Michael Mandel found these flows to have increased by 49% over the period while trade in goods and services simultaneously grew by only 2.4%.<sup>16</sup> Furthermore, Frontier Economics estimates that about half of all UK trade in services is enabled by digital technologies and their accompanying data transfers. As the services sector accounts for almost 80% of UK GDP and UK services exports account for about £123 billion or 6.9% of the UK GDP, then it follows that about 3% of UK GDP is directly affected by (or directly dependent on) the transfer of data.<sup>17</sup> We shall describe such trade activities 'data trade'.

Despite discussions as to whether the World Trade Organisation (WTO) should function as a forum for the establishment of international data trade and data protection rules, the issue remains contested. Supporters say that a WTO-based solution would resolve many issues, as international trade tends to be a very effective medium for the diffusion of policy practices. However, critics argue that global data protection norms would be very difficult to agree at the WTO-level; data privacy tends to be a politically charged issue with social, historical and cultural factors influencing it and, in turn, diverging legal approaches amongst member states.<sup>18</sup> To date, the most comprehensive Free Trade Agreement (FTA) pertaining to data transfer arrangements was the Korea-US (KORUS) bilateral agreement of 2011, which, in conjunction with other e-commerce arrangements, included a commitment of the two parties to

12 Teshuva Ariel, Why Has the EU Made So Few Adequacy Determinations?, Lawfare, 2 January 2017. <https://www.lawfareblog.com/why-has-eu-made-so-few-adequacy-determinations>

13 OECD "Internet Economy Outlook 2012" OECD Publishing [http://www.keepeek.com/Digital-Asset-Management/oced/science-and-technology/oced-internet-economy-outlook-2012\\_9789264086463-en#.WSYM\\_VKQ1mA#page1](http://www.keepeek.com/Digital-Asset-Management/oced/science-and-technology/oced-internet-economy-outlook-2012_9789264086463-en#.WSYM_VKQ1mA#page1); Meltzer, Joshua Paul. "The Internet, Cross-Border Data Flows and International Trade." Asia & the Pacific Policy Studies 2.1 (2015): 90-102.

14 McKinsey Global Institute, "Digital Globalization: the New Era of Global Flows", 2016. <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

15 Aaronson, Susan Ariel, "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", 2015.

16 Mandel Michael, "Data Trade and Growth", 2014. Progressive Policy Institute. [http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel\\_Data-Trade-and-Growth.pdf](http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf)

17 Frontier Economics, "The UK Digital Sectors After Brexit". <http://www.frontier-economics.com/de/documents/2017/01/the-uk-digital-sectors-after-brexite.pdf>, 6.

18 Asinari, María Verónica Perez. "The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection

'endeavor to refrain from imposing or maintaining unnecessary barrier to electronic information flows across borders'.<sup>19</sup> The Trans-Pacific Partnership (TPP) and the Trans-Atlantic Investment and Partnership (TIP) multilateral agreements were meant include similar provisions, however, at the time of writing both agreements appear

to be all but completely scrapped.<sup>20</sup> Thus there appears to be an alarming absence of data related arrangements in substantive WTO agreements, which, in turn, allows for all manner of governmental regulations and restriction on data transfers, ranging from economic to politically motivated ones.<sup>21</sup>

## WTO Rules on Free Data-Trade

Despite the lack of relevant commitments in international agreements, there could be another way to encourage freer data flows through the WTO. This is by invoking two of the most salient principles of the institution.

The first is the 'Most Favoured Nation' (MFN) principle, which states that WTO members are expected to extend to each other "treatment no less favourable" than that they show to their most "favoured" trading partner. The second principle is that of "national treatment", through which members pledge not to discriminate against foreign product or service providers in their national markets, and to thus treat them equally to their nationals.

Thus these principles could be invoked when a member state is restricting data flows to and from another member state, whilst not doing so for other members. Or when restricting data flows of a foreign-owned local business, whilst allowing greater freedoms for locally owned businesses, i.e. when a member state discriminates against another.

However, these principles may not be enough to ensure a the free flow of data between members under relevant agreements. There is a list that accords member states with general exemptions from market access and national treatment commitments in Article XIV of the General Agreement of Trade in Services (GATS). The aim of these exemptions is to 'protect public morals, public order or other significant societal interests, so long as those measures are not disguised restrictions on trade in services'.<sup>22</sup> Regarding personal data protection in particular Article XIV(c)(ii) states that 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts . . .'.<sup>23</sup> To date this exception has not been tested by a dispute resolution panel, nor has it attracted much attention in the GATS negotiations. Thus, the circumstances under which data restrictions are not justified under Article XIV remain uncertain, and so is a potential challenge to data discriminatory activities that may violate WTO's MFN or national treatment principles.

---

within the WTO e-commerce Context?." 18th BILETA Conference: Controlling Information in the Online Environment. 2003.

19 US Government, "KORUS FTA" Korea-United States Free Trade Agreement, Article 15.8, Electronic Commerce/Cross-Border Information Flows. [https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset\\_upload\\_file816\\_12714.pdf](https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf).

20 Meltzer, Joshua Paul. "The Internet, Cross-Border Data Flows and International Trade." *Asia & the Pacific Policy Studies* 2.1 (2015): 90-102.

21 *Ibid.*

22 MacDonald, Diane, and Streatfeild, Christine, "Personal Data Privacy and the WTO." *Houston Journal of International Law*. 36 (2014): 625.02\_e.htm

23 WTO, "General Agreement on Trade in Services", 1995. [https://www.wto.org/english/res\\_e/booksp\\_e/analytic\\_inde](https://www.wto.org/english/res_e/booksp_e/analytic_inde)



## Data trade as a global phenomenon

For more than forty years now, international trade has undergone a continuous transformation that has irreversibly disrupted traditional perceptions of the workings of international trade and the benefits of distribution of trade between different countries, as a result of the rise of Global Value Chains (GVCs).<sup>24</sup> Following the introduction of GVCs, imports have become exports and exports have become imports. Countries have been increasingly importing a significant part of the raw materials and equipment required for the production of various products and the provision of various services (both for local use, but also for exporting activities). The opposite is also true as, a significant portion of UK exports have become part of the production and service provision processes of firms in other countries.

Development of digital technologies, and data transfers specifically, have not only been vital enablers and catalysts of this process, they have also become part of it.<sup>25</sup> An estimated 49% of the UK's digital sectors rely on imported goods and services as intermediaries in their product or service delivery structures. An even more pronounced metric of how integrated UK digital businesses are in GVCs, is ownership. About two thirds of the UK information services industry GVA is estimated to come from foreign-owned firms (compared to 29% for the economy as a whole).<sup>26</sup> When it comes to UK-owned digital firms operating abroad the scene is dominated by the EU market with 81% of digital-producing firms operating in the EU and 44% of the global revenues of digital-producing firms coming from the EU.<sup>27</sup>

---

24 OECD WTO UNCTAD, "Implications Of Global Value Chains For Trade, Investment, Development And Jobs", G20 Leaders Summit, St. Petersburg (2013).

25 Palmisano, Samuel J. "The globally integrated enterprise." *Foreign affairs* (2006): 127-136.

26 Frontier Economics, "The UK Digital Sectors After Brexit". <http://www.frontier-economics.com/de/documents/2017/01/the-uk-digital-sectors-after-brex-it.pdf>.

27 EuroStat Database, 2016. <http://ec.europa.eu/eurostat/data/database> ; Frontier Economics, "The UK Digital Sectors After Brexit". <http://www.frontier-economics.com/de/documents/2017/01/the-uk-digital-sectors-after-brex-it.pdf>, 6.



# **A tale of two countries**

Data protection regulation  
in the UK and US

This chapter explores the similarities and differences of data protection regulation in the US and UK both in approach and application. The focus is primarily on the size of respective data economies, legislation, enforcement, data trade and Brexit. The US has been chosen as a case-study, not merely given the historical and cultural lineage binding it to the UK, but also to explore a country more partial to allowing business to inform regulation. Further, the US has not technically been deemed 'adequate' by the EU as a country fit to transfer personal data, however continues to trade with Europe initially through the Safeharbor arrangements and now with Privacy Shield. This arrangement makes the US an informative case study to foresee the UK's position following negotiations with the EU. Such a comparison is made yet more salient, as the Anglo-American special relationship enters new territory once the UK leaves the EU and the possibility of a trade agreement becomes all the more imminent.

### Why is the US data economy significant?

The US data economy is the largest worldwide and hence possibly holds the largest potential for UK businesses contemplating overseas expansion.<sup>28</sup> At €129 billion (£116.3 billion), the US data market is more than twice the size of the EU's €59.5 billion and almost ten times larger than the UK's (€13 billion). In addition, growth estimates show that in 2016, the US data market grew at 11.8% a considerably faster rate than the EU 9.5% and slightly lower than UK's 13.2%.<sup>29</sup>

The US market appears to be significantly more competitive than its European counterparts. The US accounts for approximately one-third of global ICT spending, while it is estimated that the US accounted for about 45% of the 2014 worldwide spending in business analytics software. Moreover, it is expected that by 2019 more than 50% of the big data and business analytics revenue will come from the US.<sup>30</sup> The US also leads in sheer number of data companies, with IDC estimating that, in 2015 there were more than 289,556 US data companies (13.6% more than those of the EU and 140% more than those of the UK). Finally, the US direct and backwards-indirect impacts of the data economy are about twice those of the EU, indicating that US data products and services are not only more advanced, but also better diffused.<sup>31</sup> Consequently, the US data economy is not only more sizeable, but faster growing and more mature than the UK and EU overall. This presents a rather

mixed picture regarding the ideal direction for a post-Brexit data regulatory framework, as entering the US market would involve both opportunities and threats. This report will go into more depth on this trade-off in the next chapter, where the possibility and content of a UK-US trade agreement will be considered in more detail.

### Contrasting US and UK approaches to privacy legislation

Given both countries' reliance on data related services to prompt economic progress, it is unsurprising that the privacy legislative agenda is ever-evolving. Despite the US and UK's use of contractual law, at first glance the two countries have contrasting approaches to data protection legislation. The UK operates under a strict data regulatory framework since the Data Protection Act of 1998 and will continue to do so under GDPR. By contrast, in the US there is no single, comprehensive federal law regulating the collection and use of personal data.<sup>32</sup> Instead, the US adopts a sectoral, post-hoc approach, allowing injured parties to bring legal action when facing 'unfair or deceptive' business practices.<sup>33</sup> When assessing respective parties' legislative approaches, many observers fail to consider that more liberal states such as California have adopted the role of pathbreaker in the data protection sphere.<sup>34</sup> California's influence in paving the way for regulation is undoubtedly 'due to its large market and preference for strict consumer and environmental

28 There are of course additional reasons for choosing the US Data Economy as a case study, these include: similarities in terms of judicial proceedings, existing business relations, existing political relations, ease of linguistic communication etc.

29 IDC Europe, "The European Data Market Study: Final Report" (2017). <http://www.datalandscape.eu/study-reports>

30 IDC "Worldwide Black Book Pivot Table", 2016, IDC, (2016). <https://www.idc.com/getdoc.jsp?containerId=US41686816>

31 Cattaneo, Gabriella, Mike Glennon, Rosanna Lifonti, Giorgio Micheletti, Alys Woodward, Marianne Kolding, and David Osimo. European Data Market Study, Second Interim Report: The Data Market in the World. Luxembourg: IDC, 2016. <http://www.datalandscape.eu/study-reports>; IDC Europe, "The European Data Market Study: Final Report" (2017). <http://www.datalandscape.eu/study-reports>

32 "Data Protection in the United States: Overview," Practical Law, 2016. <http://uk.practicallaw.com/6-502-0467>.

33 Alan Charles Raul, *The Privacy, Data Protection and Cybersecurity Law Review*. London: Law Business Research, 2014, 268.

34 Raul, *Privacy, Data protection and Cybersecurity Law Review*, 269.

regulations, California is, at times, effectively able to set the regulatory standards for all other states.<sup>35</sup> Though this phenomenon is widely accepted by academics and has been termed the “California Effect”, existing scholars have recognised the importance of market size and scale economies as a source of a jurisdiction’s external regulatory clout, without acknowledging factors such as regulatory capacity and inelasticity as key components of the theory.<sup>36</sup> Digital Catapult has discovered that particularly in the realm of data regulation, California’s influence is unparalleled to that of its forty-nine counterparts. Therefore, it is not sufficient to assess US privacy laws as a monolith and more can be learnt by analysing the approaches of California, as they trickle down to other states with a few years of delay.

In the following chapter the strengths and weaknesses of both regulatory regimes are examined, in order to offer the most viable suggestions to benefit UK. There are several laws which inform US data protection legislation, of which the main laws include: The Federal Trade Commission Act, the Financial Modernisation Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act and the HIPAA Omnibus Rule. These function across different sectors to provide varying levels of data protection for different services.

Despite the overlap and contradictions borne out of a sectoral approach in the US, there are many benefits to this system. Such a regime tends to favour business and innovation for three reasons. Firstly, most businesses observe self-regulatory guidelines, in the form of “best practices,”<sup>37</sup> which are laid out by industry leaders. Businesses are therefore encouraged by industry norms to evolve their data protection practices. Simultaneously, their counterparts’ adherence to standards prompts an increased level of competition than in the UK and the rest of the EU respectively. Secondly, laws at a state level grow each year, given their predominance over federal legislation.<sup>38</sup> Having different laws for each region of the country, allows legislation to coalesce around different sectors accordingly. Thirdly, though not universally acknowledged, some US academics such as Alan Charles Raul argue that ‘the United States’ commercial regime is arguably the oldest, most robust, well developed and

effective in the world.<sup>39</sup> This statement can only be substantiated when we examine California, Massachusetts and New York, but not when assessing the country as a whole. However, given those states’ predominance and ability to create norms, perhaps they are more revelatory of the future direction of privacy law in the US. Finally, the fourth and most important strength of the US legislative approach, breach notification. Breach notification will form an integral element of the GDPR in 2018, however as early as 2003, California required that companies notify individuals whose personal information was compromised.<sup>40</sup> California’s insistence on breach notification even prior to GDPR, highlights its ability to influence regulatory landscape, even outside of the US. Therefore, an ad-hoc developmental approach does not necessarily compromise individuals’ rights to privacy. This is particularly the case, given America’s ‘overarching and very powerful norm for consistency across decisions and to avoid deviating from prior decisions.’<sup>41</sup> Such legal precedent only functions when businesses abide by industry norms set by their competitors.

Despite the benefits of a developmental approach, the US data regulatory regime suffers from three main weaknesses. Firstly, there are inevitable gaps to adopting a “patchwork approach” and congressional action to enact comprehensive data protection legislation would substantiate the regime. Though there is bi-partisan congressional support for the protection of privacy, neither party have been willing to overhaul the current system in recent years. The American legislative approach and favouring of best practices can lead to increased ambiguity. Gaps are more likely to emerge in a system based on norms and precedent. It is far easier for the both the government and businesses to abuse privacy laws when merely a sketch is provided rather than a congressionally backed legislative agenda. Secondly, despite America being adamant that privacy is enshrined within the US Constitution,<sup>42</sup> the federal government has a history of infringing on the rights of citizens in the name of national security.<sup>43</sup> The most prominent example of this can be found in the Snowden revelations of 2013, which contained allegations of widespread surveillance of Internet data by the US intelligence

---

35 Anu Bradford, “The Brussels Effect”, *Northwestern University School Law Review* (2012), 5.

36 *Ibid.*, 7.

37 “Data Protection in the United States: Overview,” *Practical Law*, 2016.

38 *Ibid.*

39 Raul, *Privacy, Data protection and Cybersecurity Law Review*, 268.

40 *Ibid.*, vi.

41 Woodrow Hartzog and Daniel J. Solove, “The Scope and Potential of FTC Data Protection,” *George Washington University Law School* 83, no. 6 (November 2015), 2262.

42 Martin Weiss and Kristin Archick, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*. Washington DC: Congressional Research Service, 2016, 3.

43 Jamie Carter, *How to Handle the New US-EU Data Regulations*, (TechRadar), May 23, 2016. <http://www.techradar.com/news/internet/how-to-handle-the-new-us-eu-data-regulations-1320554>.

agencies and were contested by Maximilian Schrems<sup>44</sup> (as discussed in the following chapter). It is without question that the judgment is based on a condemnation of US intelligence gathering practices and their effect on fundamental rights under EU data protection law.<sup>45</sup> In the US, concerns for national security predominate over citizens' civil liberties, European or otherwise. However, we cannot forget that US concern for national security is garnered by fear of terrorist attacks and cyber-attacks perpetrated against the United States in recent years. Lest such attacks desist, neither will the protectionist attitude to US national security. Thirdly, the ambiguity borne out of the lack of a horizontal system of data protection, creates issues for trade simultaneously. As described in the previous chapter, the US is merely deemed adequate by the EU, as long as companies abide by special safeguards guaranteeing the security of European citizens' data. Most notable of these, is the Privacy Shield, which functions in the form of a self-certification system. The Umbrella Agreement is also worth noting, as that pertains to EU-US law enforcement cooperation. It is uncertain whether they go far enough to stand up to legal challenges by the Court of Justice of the European Union (CJEU),<sup>46</sup> as they have come under considerable criticism in Europe, but have been deemed too stringent in the US. This reiterates the possible irreconcilability of two countries' regulatory attitudes. Special safeguards cannot sufficiently allay contrasting perspectives on data protection.

### Strengths and weaknesses of implementing GDPR in the UK

GDPR will apply to the UK in May 2018. Currently being implemented in the UK domestic laws through the UK Data Protection Bill, published on the 13th September 2017 and currently in passage in The House of Lords. The main benefits of this new regulation are rooted in the aim of placing the individual consumer at the helm. As already established, breach notification was a Californian codified norm. However, insistence on data portability and permitting the so-called 'right to be forgotten' (right to erasure) push the boundaries of data protection yet further. Data portability would modernise the system substantially and increase consumer ease of experience. The right to erasure marks the most radical departure, as it acknowledges the desire of many to maintain anonymity in the digital domain. These newly prescribed measures will prove difficult to navigate in the coming months, however they provide an opportunity to re-evaluate business' role in providing civil assurances to consumers. This opportunity can then, Digital Catapult believes,

be nourished to increase customer trust. These three new concepts together – greater control by the individual, data portability and right to erasure - will provide the UK data regulatory regime with international acceptance and prompt a move closer to harmonisation with Europe. We have seen the difficulty in the US advocating its privacy approach without the firm boundaries detailed in a federal act or regulatory framework such as GDPR. If the UK were to adopt GDPR for a time and then heavily modify legislation upon departure from the EU, international acceptance could be rescinded and less harmonisation could cause confusion. Similarly, such a switch would lead to many businesses incurring transition costs, as they would be forced to readapt business practices and protocol all over again.

However, there are three central weaknesses borne out of the rigid format promulgated under GDPR. Firstly, the ever-increasingly rapid evolution of business and technologies are in direct contrast to the slow progress of data legislation. The simple fact that we must



44 Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems." German Law Journal 14 (2016), 5.

45 *Ibid*, 13.

46 Weiss and Archick, U.S.-EU Data Privacy, 12.

wait until 2018 to enforce this legislation, is reiterative of this slow approach to privacy law. By contrast, the US is able to codify new norms which are developing on a monthly basis. Therefore, the approach is stilted in developing legislation at a federal level in the US, however rapid in setting precedents when necessary by sector and state. By contrast, the EU system is unable to stay up to speed with the technology sector. Secondly, the UK's legal system is based on precedent decided in the courts by regulators. The system operates with a body of case law, which sets out what the rules are from the outset. Such a system is contrary to many European systems' use of civil law. This difference in legislative approach will be further intensified by the fact that UK public authorities will not be subject to the Court of Justice of the European Union (CJEU) or European Data Protection Board (EDPB), which are quintessential elements to enforcing GDPR. The EDPB is to take over the activities of the Article 29 Working Party, the body made up of member states which provides expert advice on data protection and set the terms of GDPR.<sup>47</sup> However, as the EDPB will be an independent body of the EU and its chief remit will be to contribute to the consistent application of the GDPR,<sup>48</sup> such a role cannot be taken on in the UK. Finally, the UK's influence on a regulation as broad as the GDPR is also restricted given other members' conflicting objectives. This report will come to explore this further, but it is safe to say that Brexit coupled with the implementation of GDPR will present a scenario whereby the UK simultaneously implements and loses the ability to influence a data regulatory regime dominated by the EU.

## How the US and UK enforce privacy legislation

The US and UK systems of enforcement are equally divergent to the legislation we have discussed thus far. The Information Commissioner's Office (ICO) has the clearly defined role of official enforcement regulator in the UK. The ICO charges itself with 'taking action to change the behaviour of organisations and individuals that collect, use and keep personal information.'<sup>49</sup> By contrast, there is no top-level privacy regulator or coordinator in the US.<sup>50</sup> In fact, the Federal Trade Commission (FTC) has taken on the role of de-facto

privacy enforcer, defining its role as 'the nation's consumer protection agency.'<sup>51</sup> The FTC's most clear mention of privacy is in stating that it 'works to prevent fraudulent, deceptive and unfair business practices in the marketplace.'<sup>52</sup> Herein lies yet again the key distinction between the US and UK data regulatory regimes. In the UK, there is a clear assertion of intent to protect privacy even prior to GDPR coming into effect. The US's reluctance to clearly assign a body to enforce privacy legislation makes it difficult for it to 'explain and advocate for its approach to protecting personal information.'<sup>53</sup> However, to completely discount US enforcement completely is also misleading.

There are several strengths to US data legislative enforcement. As we have seen, the US operates data regulation with a sectoral emphasis. Similarly, enforcement is not simply carried out by the FTC, as state attorney generals and private plaintiffs are equally important in enforcing privacy under analogous 'unfair and deceptive acts and practices' standards in state law.<sup>54</sup> Perhaps this three-part ecosystem of enforcement is merely yet another difference in attitudes to data protection and not a sign of weaker a data regulatory regime. The FTC can go as far as initiating an investigation, issuing a cease and desist order, and filing a complaint in court.<sup>55</sup> This highlights the FTC's strength in privacy law's enforcement, which is simultaneously reinforced by state attorney generals and private litigation. So long as all three unofficial bodies are diligent in their roles, they are able to exert their power significantly and protect consumer interests. Another benefit to this nimble approach to data regulatory enforcement, is that broad definitions such as 'unfair or deceptive acts or practices' can be developed further and evolve as time goes on to suit the privacy landscape as it changes. The number of companies using personal data will continue to increase significantly as emerging technologies rise in importance. Therefore, it is beneficial for an enforcement body to be able to interpret broad definitions differently depending on what the privacy landscape prioritises. Motives and objectives must be in line with the FTC in order for the system to function.

However, with this flexibility, comes a lack of clarity, which create several damaging elements to this system of enforcement. Enforcement is dependent on all three levels of the privacy ecosystem

---

47 Craig Richard, "The 'one stop shop'" TaylorWessing, April 2016. <https://united-kingdom.taylorwessing.com/globaldatahub/article-the-one-stop-shop.html>.

48 *Ibid.*

49 Information Commissioner's Office, "Taking Action - Data Protection," December 8, 2016. <https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/>.

50 Raul, Privacy, Data Protection and Cybersecurity Law Review, vi.

51 Federal Trade Commission, "Privacy, Identity & Online Security | Consumer Information". Consumer.Ftc.Gov, 2017. <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

52 *Ibid.*

53 Raul, Privacy, Data Protection and Cybersecurity Law Review, vi.

54 Raul, Privacy, Data Protection and Cybersecurity Law Review, 272.

55 "Data Protection in the United States: Overview," Practical Law, 2016.

working in tandem. This is not always possible given the possibly divergent priorities for each enforcement body. With this lack of clarity, comes an ability to cheat an enforcement system dependent on mutual cooperation. Even more important, however is the fact that broad definitions of the FTC's role, make it difficult to assess when it is pushing its boundaries and when it is not going far enough. In fact, some critics contend that the FTC is engaging in a form of rule-making in this area when it lacks meaningful rule-making authority.<sup>56</sup> While others are adamant that the FTC should be asserting its influence to a much greater degree, provided that the agency also becomes more transparent in its enforcement and more willing to use a mixture of carrots and sticks.<sup>57</sup> The wide range of opinions on the FTC's enforcement capabilities highlight the extent to which the body's power is not clear enough.

By contrast, UK data protection enforcement is widely recognised for its pragmatism. There is a recognition among the ICO that personal data will be needed to prompt innovation and technological advancement. By working on this basis, the ICO uniquely works with business and consumers to deal with hundreds of thousands of complaints per year. Anecdotally the ICO has a reputation for being hard, but fair in its approach; by contrast its French and German counterparts have earned the reputation of being so strict as to stunt data innovation.

There are two primary difficulties arising from the future enforcement of GDPR by the ICO. Firstly, the regulation is extremely complicated and small businesses will find it hard to comply. Despite precision in articulating broad concepts, the GDPR is extremely unclear in detailing certain terms. Words such as 'high risk', 'substantial effects', 'large scale' and 'systemic' do not clearly define the boundaries of DPAs' reach. For example, when discussing sensitive, personal data the GDPR describes the need to prevent 'significant risks to the fundamental rights and freedoms.'<sup>58</sup> However, perception of 'significant' will vary from person to person. Similarly, when discussing supervisory bodies' power, the GDPR refers to 'matter does not substantially affect or is not likely to substantially affect'<sup>59</sup> Yet again how can one measure substantial effects, as subjectivity comes into play. The concept of 'processing, on a large scale,'<sup>60</sup> is also continuously introduced, which also creates ambiguity. Such terms will be interpreted differently depending on the business, which will be difficult for the ICO to assert its authority. It is harder for the ICO to determine what to do and when to do it under GDPR. The second difficulty is linked to the first and also to the legislative issues outlined previously. It is already evident how much white space is left to be filled in by the CJEU and EDPB, however it is unclear how these two enforcement bodies will successfully work to substantiate the ICO, given Britain's exit from the EU.

---

56 Hartzog and Solove, "The Scope and Potential of FTC Data Protection," 2232.

57 *Ibid*, 2300.

58 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) <http://data.europa.eu/eli/reg/2016/679/oj>, 10.

59 *Ibid*, 24.

60 *Ibid*, 15.



# Opportunities and risks for the UK data economy post-Brexit

Four scenarios



This chapter analyses the opportunities and risks for the UK with a particular focus in personal data data market post-Brexit. The main topics under consideration include: the EU Digital Single Market, the free movement of data, adequacy, localisation, the impending EU-UK trade deal and the possibility of a US-UK bilateral agreement. It then provides an in-depth analysis of four extreme scenarios, posed in order to assess the main opportunities and risks that each could prompt. This is followed by an outline of what the UK should strive towards obtaining and effectively describe the “ideal scenario” for the UK data economy.

## The Digital Single Market in Europe

The creation of a Digital Single Market has for long been on the European Commission’s agenda and was a main campaign pledge of the current Commission’s presidency in the run up to the 2014 election. This intention first materialised in the “Digital Single Market Strategy for Europe”, issued in 2015.<sup>61</sup> In general, the Digital Single Market holds three goals:

1. Better access for consumers and businesses to digital goods and services across Europe.
2. Creating the right conditions and a level playing field for digital networks and innovative services to flourish.
3. Maximising the growth potential of the digital economy.

The UK government has also been a supporter of the creation of a European Digital Single Market, particularly enabling greater free flow of data, whilst maintaining data restrictions relating to national security and law enforcement needs. It is estimated that there will be a £308 billion increase in EU GDP through the creation of the Digital Single Market; Digital Catapult suggests that a disproportionate part of this value increase could go to the UK (assuming UK businesses maintain full access to the Digital Single Market post-Brexit).<sup>62</sup> As we increasingly live in a digital and data dependent economy, there has been broad consensus amongst European stakeholders that the effective functioning of the EU Single Market necessitates the creation of a Digital Single Market.

Today this initiative has taken the form of a series of white papers, updates of existing directives and relevant consultations by the European Commission aiming to enable a discussion with stakeholders to lead to the shaping and eventual introduction of a Digital Single Market by spring 2018 (the same period as the introduction of GDPR).<sup>63</sup> A frequently cited example of an issue to be addressed by Digital Single Market, is “geo-blocking”, where some digital services, akin to Netflix, Amazon Prime, Spotify etc., are not available for the European consumer should she travel to another EU country (besides the one where the purchase was initially made). But with regards to the economic opportunities created for UK data businesses, perhaps the most important of the Digital Single Market initiatives is the Communication for ‘Building a European Data Economy’.<sup>64</sup>

## The free movement of data within Europe

The overall goal of the European Data Economy initiative’s is ‘to tackle restrictions on the free movement of data for reasons other than the protection of personal data within the EU and unjustified restrictions on the location of data for storage or processing purposes’ and to ‘use EU trade agreements to set rules for e-commerce and cross-border data flows and tackle new forms of digital protectionism’.<sup>65</sup> Therefore, there is a clear consensus that practices of private and public bodies in Europe in conjunction with a relatively anachronistic policy framework, are hindering the potential of the Single Market to properly use data and its value creating potential.

61 European Commission, “A Digital single Market Strategy for Europe”, 2015. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>; <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>

62 European Commission, “The Digital Economy and Society Index”, 2017, <https://ec.europa.eu/digital-single-market/desi#desi-scores-by-dimension>; Traynor Ian, “EU Unveils Plans to Set up Digital Single Market for Online Firms”, The Guardian, May 6, 2015. <https://www.theguardian.com/technology/2015/may/06/eu-unveils-plans-digital-single-market-online-firms>

63 European Commission, “e-Commerce Directive”, 2015 <https://ec.europa.eu/digital-single-market/en/e-commerce-directive>; European Commission, “Proposed Directive establishing the European Electronic Communications Code”, 2015.

64 European Commission, “Staff Working Document on the Free Flow of Data and Emerging issues of the European Data Economy”, 2017 <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>.

65 European Commission, “Communication on Building a European Data Economy”, 2017. <https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>

Furthermore, lack of relevant rules in trade agreements also hinder the potential that data hold for EU trade with third countries. Thus this communication aims to form a basis for discussion to address these issues. The European Commission advocates for the creation of a clear legal and policy framework around data, the removal of barriers to the movement of data and addressing uncertainties around new technologies. In particular, the communication focuses on 'free flow of data; access and transfer in relation to machine-generated data; liability and safety in the context of emerging technologies; and portability of non-personal data, interoperability and standards'.<sup>66</sup>

Given the UK has by far the largest number of data companies in Europe, along with a leading position in data revenue earnings, high ICT spending and data openness, the Digital Single Market could disproportionately benefit UK tech firms by giving them room to scale, with an ease that is only comparable to other big tech markets, such as China and the US. Therefore, there will be a better chance for UK-based start-ups to develop to fully-fledged multinationals, an economically and politically desirable goal. In addition, the UK creates a larger volume of data flows than any other European economy, which hints to disproportionately significant benefits from the Digital Single Market through greater and faster flows and data trade. Conversely, not being able to access the Digital Single Market presents a significant risk for the data economy. Given Brexit, the extent to which UK data businesses will be able to reap the potential benefits of the Digital Single Market, remains a matter for the future UK-EU exit negotiations and the subsequent trade agreement.

## The importance of the UK achieving adequacy

Adequacy is one of the greatest areas of uncertainty surrounding Brexit. On the basis of Article 25(6) of Directive 95/46/EC, the Council and European Parliament have given the European Commission power to determine whether a 'third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into'.<sup>67</sup> Obtaining adequacy allows personal data to flow to that third country without any further safeguards. At this time, merely eleven countries have been deemed adequate. These countries include Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States (so long as companies abide by the Privacy Shield). Whether the UK will be deemed adequate is difficult to ascertain, particularly given the lack of a clear thread running through the 'adequate' countries listed above. We have already observed that GDPR will be implemented in the UK based on the Prime Minister's statements. Logically, even if the UK's regulatory regime diverges on all of the thirty-three flexible derogations, adequacy should not be an issue. However, replication of GDPR does not necessitate adequacy. There are several other considerations such as national laws and security. Further, the recent replacement of The Data Retention and Investigatory Powers Act 2014 with the Investigatory Powers Act 2016 has tempted criticism by both domestic politicians and the UK's European counterparts. But it is difficult to determine whether this could go as far as preventing adequacy.

The process of obtaining adequacy as defined by the Article 29 Working Party is as follows:

- "A. Processing should be based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;
- B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed (generally national security) and the rights of the individual;
- C. An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;

<sup>66</sup> European Commission, "Staff Working Document on the Free Flow of Data and Emerging issues of the European Data Economy", 2017. <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>

<sup>67</sup> European Commission, "Commission Decisions On The Adequacy Of The Protection Of Personal Data In Third Countries - EC", Ec.Europa.Eu, 2017, [http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).

D. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body.”<sup>68</sup>

Surprisingly, there are several reasons by the UK not being deemed ‘adequate’ by the European Commission may not be cause for grave concern. Firstly, adequacy is merely one way of making an international transfer. The alternatives include model clauses (standard EU clauses) and binding corporate rules. Secondly, while the UK has been a member of the EU, its main trading partners (US, Brazil and Japan) have not been deemed adequate by the Commission. However, this has not impeded on trade significantly. Finally, special safeguards can also serve as an alternative to adequacy determination. In fact, the US is not technically considered adequate, but operated under Safeharbor and now the Privacy Shield, in order to safeguard EU citizens’ privacy entitlements. As explored in the previous chapter, it is important to note that if deemed inadequate, the UK could very well find itself developing a special safeguard to supplement its regulatory regime.

On the other hand, the transfer of personal data across national borders has become crucial for social interaction, economic growth and technological advancement.<sup>69</sup> Therefore, the importance of the UK obtaining adequacy cannot be ignored for several reasons. Firstly, the alternatives to adequacy listed above (binding corporate rules and model clauses) can create many difficulties in allowing the flow of data to a country. Both require a separate set of contracts for each individual transfer of data, which can prove to be very impractical. Secondly, if the UK is deemed inadequate and trade negotiations go badly for the UK, the EU can threaten to block transfers to the UK. Though this is an unlikely scenario, it remains a possibility that should be considered nonetheless. Should the UK adopt laws antithetical to the EU’s simultaneous trajectory, the EU could very well pursue a punitive course and make data transfers very difficult for the UK. By the same token, EU data protection authorities (DPAs) have the power to block flows of data to the UK if the UK is deemed inadequate. In 2015 it was confirmed that DPAs can examine the level of data protection in a third country of their own accord and their role was strengthened at the expense of the Commission.<sup>70</sup> Again this is unlikely given the UK’s continued trade with both Brazil and Japan, despite their inadequacy. However, this very grave possibility cannot be ignored. Thirdly and most importantly, even if the UK is able to transfer data through special safeguards, many difficulties are borne out of an at times ambiguous arrangement.

The Maximilian Schrems v. Data Protection Commissioner is the most obvious example of the difficulties of supplementing regulation with special safeguards. This decision is widely acknowledged as ‘a landmark case that strengthens the fundamental right to data protection in EU law.’<sup>71</sup> As mentioned previously, Schrems brought to light the limitations of US safeguard, Safeharbor. This legislation has been replaced by the Privacy Shield, which despite much discussion in creating it, has still come under considerable criticism. Therefore, special safeguards cannot necessarily satisfy privacy concerns long-term. Despite UK proximity to the EU, there is no way of assuring that if deemed inadequate, the UK’s special safeguards would be any more accepted than those of the US.

### The risk of localisation for the UK post-Brexit

As stated above, creation of the Digital Single Market is a multifaceted endeavour, involving a variety of policy issues. Digital Catapult has sought to identify the most prominent Brexit related risk for UK data businesses, which it sees as ‘localisation’ of data. Localisation has emerged as an important risk as it was found to cause a clear practical complication for doing business in the Digital Single Market. This observation surfaced both through our literature review and is a primary Brexit concern for many of the data businesses that were interviewed.

In its simplest form localisation refers to the requirement that a firm maintains its data, and hence related facilities and personnel in the market, country and regulatory space where it operates. There is a clear threat of increased costs and opportunity costs from a potential post-Brexit localisation of UK data-businesses that currently operate in the EU, or that have future plans for expansion into the EU Digital Single Market. There are three main reasons for this that have emerged from both the secondary research as well as the interviews with businesses (discussed in Chapter 4). The first, and most likely reason localisation could be a threat, is that of an increase in legal costs.<sup>72</sup> Extra legal arrangements will have to be made both in terms of contracts, as well as regulatory compliance, in order for UK data businesses to ensure that they meet data privacy and data transfer standards. Businesses will have to draw relevant contractual arrangements and to adjust their data practices, depending on the EU member state their data will be stored or processed in. In turn, this is likely to drive up any associated legal costs and fees.

68 European Commission, “Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment”, Ec.Europa.Eu, 2016, [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2016/20160203\\_statement\\_consequences\\_schrems\\_judgement\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf).

69 Kuner, Christopher, “Reality and Illusion in EU Data Transfer Regulation Post Schrems.” German Law Journal 14 (2016), 1.

70 *Ibid*, 11.

71 *Ibid*, 3.

72 FrontierEconomics, “TheUKDigitalSectorsAfterBrexit”. London:2017TechUK.<http://www.frontier-economics.com/de/documents/2017/01/the-uk-digital-sectors-after-brexit.pdf>

Secondly, localisation poses a risk given the issue of increased segmentation of data storage. That is, the need to store data in multiple storage facilities (both UK and EU) will raise the costs and time of storage and processing, this, in turn, will create higher barriers to entry into the EU market, as businesses will need to build, purchase or lease relevant infrastructure from one or multiple EU members. Alternatively, firms that already operate in the EU will either be required to make additional storage arrangements in the UK or the EU to meet relevant regulatory requirements. In addition, the free flow of data to and from the UK, along with the freedom to use storage in other European countries, creates greater competition (and hence choice) for storage service provision, which in turn lowers costs for data businesses.

The third risk factor of localisation is the opportunity cost set to arise from not being able to fully leverage the value-creating benefits of centralised data processing and storage on a Pan-European level. Such innovations as Business Analytics and Cloud Networking leverage large data pools and the ability to use non-local internet-based resources, in order to provide significant benefits for businesses. This is because such technologies enable them to create further value from data and the internet by implementing more efficient IT and networking solutions. In addition, the rapid development and expansion of such new technologies as big data analytics is further increasing the benefits of centralised storage and processing. In turn, these innovations raise the associated opportunity costs of not being able to take advantage of them on the level of the EU single market.

## Brexit and the UK-EU data relationship

As stated by the government's White Paper on the 'The United Kingdom's exit from and new partnership with the European Union', the UK will not pursue membership of the EU Single Market and will instead opt for a comprehensive trade deal with the EU. It is difficult to predict the scope of this deal but it is expected that both sides will aim for an arrangement to sufficiently substitute the existing economic relationship (to the extent that this serves their individual interests). If this is indeed the case, then it is likely that the EU will for the first time in its trading history negotiate a bilateral trade deal to cover trade in services (an extremely important aspect for the UK digital and data sectors). As stated in section 8.40 of the recent Brexit white paper, the government 'intends to maintain the stability of data transfer between EU Member States and the UK'.<sup>73</sup>

Digital Catapult expects that the UK government will try to include the issue of data transfers and privacy in the discussion, either by attempting to set new relevant rules, or at least by trying to achieve some sort of clarification regarding the UK-EU data relationship.

Both the primary and secondary research conducted for this report, indicates that the general expectation, is that the negotiations will involve a "rational trade-off" in the form of the UK having less policy flexibility on data, in exchange for a lower reduction in market access and vice-versa (in Figure 1 a rational agreement should gravitate around a straight line between quadrants 1 and 4). Consequently, it might seem rather unlikely that the UK obtains full autonomy to set its own data regulatory policy while maintaining full access to the EU digital market; likewise it would seem very likely that the negotiations result in autonomy levels remaining as is, whilst UK-EU data relations fall to the WTO-rules level. Any such "extreme" scenarios (Figure 1) are improbable and the end result would likely gravitate around the center of the flexibility-access matrix.<sup>74</sup> However, this report will not endeavor to predict or estimate the exact point of such a "rational trade-off", as this is not only beyond its scope, but also a rather precarious endeavor.

There are three main reasons for this:

Firstly, addressing data transfers might not be considered a salient enough topic to be included in initial negotiations after all; this, for example, could be done for the sake of achieving a quicker deal by reducing the number of topics on the table. It could also be the case that British and EU negotiators' lack of experience in negotiating data transfer issues in a trade deal setting, encourages them to underestimate or disregard the issue entirely. In general collective decision-making research illustrates that groups (and agents) are likely to "differ" taking a decision on a topic whose mechanics they do not understand very well. Data-trade fits this definition, not only given the lack of awareness amongst trade policy-makers about it, but also due to its sheer novelty and complexity.

Secondly, it might not be in the interest of British negotiators to discuss data transfers and privacy in initial negotiations. This implies neither that the issue is unimportant, nor that the UK might be better off if data remained unnoticed. Rather, it might be the case, that at least for the next two years, the data sharing relationship of the EU and the US changes and this has a direct impact on the UK's ideal negotiating position on data in the EU trade agreement.

73 UK Government, "The United Kingdom's exit from and new partnership with the European Union", [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/589191/The\\_United\\_Kingdoms\\_exit\\_from\\_and\\_partnership\\_with\\_the\\_EU\\_Web.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589191/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf) Accessed 2 February 2017, 45.

74 Putnam, Robert D. "Diplomacy and domestic politics: the logic of two-level games." *International organisation* 42, no. 03 (1988): 427-460.

There are two reasons for this. The first is the Privacy Shield. Despite significant modifications and improvements from the previous EU-US data transfer arrangement (Safeharbor), businesses, policymakers and specialists express serious concern about whether the Privacy Shield could withstand a legal challenge, arguing that it placed on shaky legal ground. If (like Safeharbor) the Privacy Shield is found to be inadequate by EU courts, then EU-US data transfers could be in jeopardy, a scenario where UK access to the Digital Single Market might be more beneficial than expected, as the UK could become the favored transfer-hub for US data to and from the EU.

Furthermore, UK negotiators might find themselves wanting to postpone making a data transfer arrangement with the EU given the Transatlantic Trade and Investment Partnership (TTIP) agreement between the EU and the US. At the time of writing, the current US administration has yet to take a position on the issue, however Robert Lighthizer has been deemed US Trade Representative. Though there have been electoral promises for a cancellation of the TTP and TTIP it appears that the US administration will not be absolute in this position, as it has stated that it has “not formulated a final position”, but what that means exactly will depend Lighthizer’s approach. With regards to the TTIP in particular, Lighthizer has stated that he would remain open to discussing addressing trade barriers with the EU.<sup>75</sup>

Of course by this logic, it could be argued that UK negotiators could postpone all the uncertain aspects of the UK-EU trade agreement, which this report does not advise as sensible nor in the general interest of the UK. However, data transfers might be an exception, given the extent to which the trade activities of the digital economy in general, and data activities in particular, are based on services. A study published by Frontier Economics calculates that 81% of the UK digital exports are in services and estimates that more than one third of them are with EU partners.<sup>76</sup> This is important given the TTIP’s ardent aims at service liberalisation. Generally, tariffs on physical goods tend to be very low among developed countries and the EU-US trade relations are no exception; thus the TTIP seeks to expand liberalisation to new areas (mainly services and investment).<sup>77</sup> Hence, the potential effect that the TTIP will have on the UK’s negotiating stance on data trade is significant and thus this is another factor that

may encourage UK negotiators to wait. Again this report does not argue that the UK might be better off delaying a discussion on data trade with the EU; the point here is that this is yet another source of uncertainty when it comes to pinpointing what an ideal compromise would be in the UK-EU data-trade negotiations.

Finally, the third source of uncertainty pertains to knowing whether the negotiated topics and trade-offs on data trade will result in an exchange in the form of “less policy flexibility for more market access” and vice-versa. It is challenging to anticipate such a development given the plurality of subjects and industries that will be involved in the negotiations, as this often presents opportunities for cross-sectoral trade-offs. Therefore, the British government might find it more beneficial to exchange its autonomy for changes to data-related legislation for better terms on an unrelated subject (say financial services passporting rights); or that the government might make a concession on an unrelated issue so as to ensure both data regulation flexibility and access to the EU data market.

Although the probability of each of the above three points, is arguably individually low, their summative likelihood is rather significant. That is, there is a fair chance that negotiators will marginalise the issue of data transfers and/or avoid including it in the initial negotiations and/or involve it in a cross-sectoral trade-off. Again this does not imply that data will not be of importance in the negotiations. Rather this explains why this report does not attempt to point to a particular point on the flexibility-to-access matrix, that is, not to set an explicit Brexit goal or strategy for data in the Brexit negotiations, as doing so will be very precarious. Alternatively, this report has opted for helping policy-makers and businesses prepare by being able to identify different post-Brexit data arrangement scenarios, and particularly by drawing attention to specific post-Brexit risks and opportunities for the UK data economy. Doing so, allows negotiators and policy-makers to be more flexible in meeting the goals they set before the negotiations; and it will be easier for business leaders to follow developments, as their focus will shift from the likely complicated and messy “overview of the negotiations” to the more ordered “status of particular risks and opportunities”.

---

75 Von Der Burchard, Hans, “Trump’s pick for trade envoy open to continued EU trade talks”, Politico, March 21, 2017. <http://www.politico.eu/article/trumps-pick-for-trade-envoy-open-to-continued-eu-trade-talks/>

76 Frontier Economics, “The UK Digital Sectors After Brexit”. London: 2017 TechUK. <http://www.frontier-economics.com/de/documents/2017/01/the-uk-digital-sectors-after-brex-it.pdf>.

77 Elliot Larry, “Brexit Britain is suddenly debating trade – but it’s the wrong talking point”, The Guardian, March 19, 2017. <https://www.theguardian.com/business/economics-blog/2017/mar/19/brexit-britain-talking-trade-deal-eu-wrong-talking-point>

Figure 3:  
Potential outcome of Brexit negotiations  
with respect to EU and US data trade

	■ US-UK	■ EU-UK
EEA-like Access	US-EU Privacy Shield Applies (No special UK-US arrangement possible)	Full Digital Single Market Access
EU-US Data Hub Status	Enhanced Privacy Shield (access to EU data market)	Enhanced Privacy Shield OR If EU-UK Arrangement allows it, a Data Trade Bilateral Agreement
Adequate Third Country Status	Privacy Shield OR Data Trade Bilateral Agreement	Data Trade Bilateral Agreement
No Deal	No Data Related Arrangement (minimal access to EU data market)	Enhanced Data Trade Bilateral Agreement (no EU adequacy constraints)

Source: Digital Catapult Analysis

## Brexit and the UK-US data relationship

Despite disparate regulatory regimes, Brexit provides an opportunity for the UK and US to strike a bilateral trade deal. Both the US and UK administrations, have openly expressed their desire for a quick deal after the UK officially exits the EU. An improved UK-US trade deal would place the UK at a more advantageous position in transatlantic trade than its European counterparts. There is much discussion in the media of the opportunity to slash tariffs and make it easier for hundreds of thousands of workers to move with increased ease between the two countries. However, as the average EU-US tariff level is at only 3%, a deal is more likely to focus on non-tariff barriers (mainly regulatory and standards harmonisation). Given America's larger market size, and hence negotiating power, as well as the sense of urgency on the UK side to establish trade relations with major markets quickly, it would be fair to say that the UK is more likely to be accommodating to US regulatory and standards preferences, which could result in regulatory changes or simply increased deregulation.

Despite continual mention of an expedient trade deal between the US and UK, at the time of writing, there has been no mention of the future of the UK-US data transfers relationship. In fact, this could be the case until the official exit of the UK from the EU. Nevertheless,

the current US administration has made clear that it aims for a prioritisation of US interests in general, which, with regards to data protection, has so far only appeared in the Executive Order for 'Enhancing Public Safety in the Interior of the United States'. Section-14 of the Order mandates US security agencies to 'ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information'.<sup>78</sup> EU (and hence UK) citizens will not be excluded from the protection of such privacy policies as the i) Privacy Shield, ii) the US-EU Umbrella Agreement (which meets the definition of 'applicable law' by being implemented through the 2016 US Judicial Redress Act), and iii) a relevant Designation made by the US Attorney General.<sup>79</sup> However, as UK citizens will most likely not have EU citizen status post-Brexit, an arrangement will be necessary for the UK government to ensure that standards of personal data protection UK citizens currently enjoy in the US remain the same. A UK-US trade deal may very well be the forum where such an arrangement is made, but what this will mean for the UK privacy regulation is yet unknown. It might be the case that the US will show the goodwill of simply extending such protections automatically with no need for any trade-off, it might also be the case that political, private, or other interests prevent or try to take advantage of this.

78 White House. "Executive Order: Enhancing Public Safety in the Interior of the United States." Office of the Press Secretary, 2017. <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>

79 McCarthy Kieren, "Trump signs 'no privacy for non-Americans' order – what does that mean for rest of us?", The Register, January 26, 2017. [https://www.theregister.co.uk/2017/01/26/trump\\_blows\\_up\\_transatlantic\\_privacy\\_shield/](https://www.theregister.co.uk/2017/01/26/trump_blows_up_transatlantic_privacy_shield/); UK Government, "UK Digital Strategy", Department of Culture, Media and Sport, March 1, 2017. <https://www.gov.uk/government/publications/uk-digital-strategy>.



However, the UK could face several risks and complications in pursuing a quick UK-US trade deal. Firstly, the issue of time is a prominent one, as EU membership prohibits engaging in actual trade negotiations with third countries (a UK-US deal can be signed in Q2 2019 at the earliest).<sup>80</sup> Secondly, it might not be in the best interest of the US to negotiate a deal with the UK without knowing whether it would serve as a gateway to the EU market. Furthermore, trade policy officials and specialists have argued that it is in the best interest of potential UK trade partners to wait until the terms and content of the EU-UK trade deal are known, so as to have a better idea of the ideal negotiating stance.<sup>81</sup> Thus it might be the case that US authorities find it beneficial to avoid taking a position on different aspects of the deal until 2019 or even later (if the an EU-UK deal is not concluded by 2019, which is quite likely). Thirdly, the inherent complexities of trade agreements (be it legal, procedural or other) mean that a 2019 deadline could be hard to achieve regardless of the above.<sup>82</sup> Fourthly, the need for the US and UK to accept each others' standards and regulations presents another additional risk and complexity.<sup>83</sup>

There could be diverging approaches on a variety of topics, from hormone usage in meat to financial and banking regulation. With regards to personal data, the difference in the US-UK legal approach to privacy (as outlined in the previous chapter), as well as differences in privacy standards and data transfer procedures, may also prove controversial.<sup>84</sup> It is thus unquestionable that such regulations would impact UK's firm values in the privacy realm. Fifth, there are political reasons for different groups in both countries not supporting such a deal. In the US, despite the presidential Fast Track Authority (under which the TTP and TTIP were negotiated under) US congress has the final say on the ratification of a trade deal; thus negotiations will have to take into consideration and appease various sectoral and geographic special interests that might be affected by a prospective trade deal. Similarly, in the UK, a trade deal with the US will have to withstand parliamentary scrutiny and be ratified by parliament. Again sectoral and geographic interests will influence parliament and hence they will have to be appeased, meaning that making a "quick" and "good" trade deal with a comparably good data-related aspect, may very well be well beyond the intentions and altruism of the US and UK governments.<sup>85</sup> Such risks form part of the curse of all trade agreements; balancing competing interests and dealing with immense questions on the part of external parties.<sup>86</sup>

---

80 Biscop Daniel, "Donald Trump: I'll do a deal with Britain". The Times, January 16, 2017. <https://www.thetimes.co.uk/edition/news/i-ll-do-a-deal-with-britain-6hl2hl73l>

81 Hanke Jacob and Mucci Alberto, Theresa May's Brexit trade bluff, Politico, April 3, 2017. <http://www.politico.eu/article/theresa-may-brexit-trade-bluff-uk-economy-negotiation-eu/>

82 Bloom, Jonty "Reality Check: Can There Be a Quick UK-USA Trade Deal?" BBC Business (BBC News), January 16, 2017. <http://www.bbc.co.uk/news/business-38639638>.

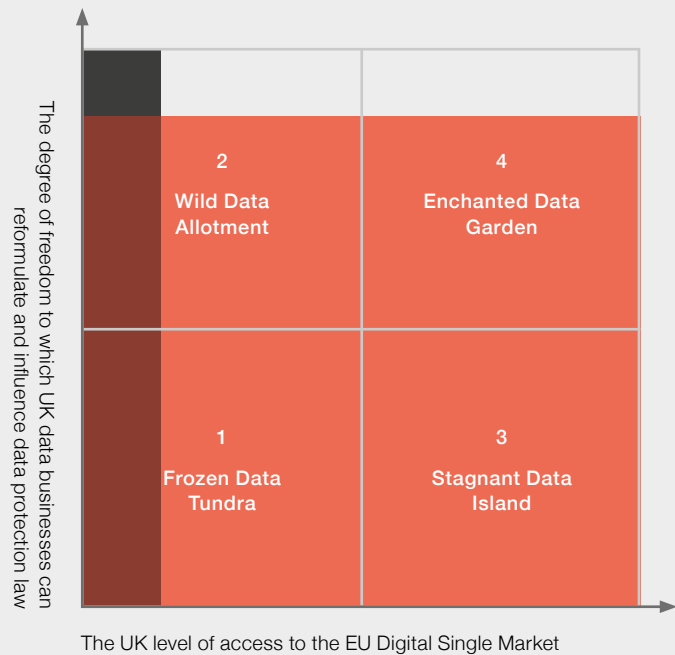
83 *Ibid.*

84 Donnan Shawn, "Trump's UK trade pledge: hurdles to a quick deal". Financial Times. January 16, 2017. <https://www.ft.com/content/378c2678-db9d-11e6-9d7c-be108f1c1dce>

85 De Bièvre, Dirk, and Andreas Dür. "Constituency interests and delegation in European and American trade policy." *Comparative Political Studies* 38.10 (2005): 1271-1296.

86 Donnan Shawn, "Trump's UK trade pledge: hurdles to a quick deal". Financial Times. January 16, 2017. <https://www.ft.com/content/378c2678-db9d-11e6-9d7c-be108f1c1dce>

Figure 4:  
Four extreme scenarios produced by Digital  
Catapult in relation to market access and data  
privacy regulation.



Source: Digital Catapult Analysis

## Four extreme scenarios as a thought-experiment

As previously stated, we assume as a baseline that the UK will not form part of the EU Digital Single Market and GDPR will be implemented in the UK in some form by May 2018. These assumptions have led us to explore two flexible variables: the UK's level of access to the Digital Single Market and the level of freedom for UK data businesses to reformulate data protection.

These assumptions have provided a springboard for the exploration of four extreme scenarios (as illustrated in the diagram above).

This report will now describe the four most extreme points of the diagram above and the opportunities and risks borne out of all four extremities. Evidently, the most realistic post-Brexit scenario will fall in the winset of probable outcomes (as shown above), however, it is still important to understand four of the most extreme possible outcomes. This allows us to identify the different directions that the post-Brexit data regulatory landscape can take and what moving more towards each of these directions implies for data businesses and for consumers.

### Scenario 1 Frozen Data Tundra

UK with no access to the Digital Single Market and imposition of GDPR with little capacity to influence regulation. The first scenario has been named "Data Tundra" to represent the permanently frozen state of data trade and data innovation, if the UK were to have neither access to the Digital Single Market nor possibilities of influencing regulation.

## Opportunities

One of the main opportunities, or at least a reduction of risk for the data tundra scenario is the stability of the UK regulatory regime with respect to the rest of Europe. The UK's imposition of GDPR without substantial modifications could be viewed as a blueprint outside Europe for other non-EU countries who nevertheless wish to market their products to European consumers and businesses. There is also the simplicity of implementing a single data protection regime for those companies targeting European consumers, as the GDPR definition of territoriality means that companies outside the EU targeting EU consumers and businesses are nevertheless subject to the regulation. (Exactly how the territorial extent of the legislation will be imposed is currently unclear.) Levels of consumer trust, the low levels of which are widely believed to be one of the key reasons why the IoT market has not developed as quickly as original forecasts, would be likely to increase under this scenario given the stringent nature of GDPR.

## Risks

The risks far exceed the opportunities in this regime. The UK's optimal conditions for both data innovation and start-up progression would quickly dissipate, as access to markets would be halted, while businesses would come second to the strict regulatory regime imposed by the EU. A drain of people with data skills would be inevitable, as other markets and regimes would prove more far more appealing than "Frozen Data Tundra." The UK would inevitably lose its status as a good destination for data and the data economy would suffer as a result.



## Scenario 2

### Wild Data Allotment

UK with no access to the Digital Single Market, but businesses are able to influence regulation. The second scenario is named “Wild Data Allotment” to represent the stilted level of access to markets compared to the rampant regulatory influence enjoyed by businesses.

#### Opportunities

If the UK to find itself in a “Wild Data Allotment” scenario, the gap between technological innovation and regulatory policy could be bridged. By the same token, companies would be encouraged to participate in industry-wide certification schemes, as they would truly feel that they had a stake in influencing the direction of data protection policy.

#### Risks

Such an extent of business predominance could result in less consumer trust that their data were not used irresponsibly. Despite ability to influence legislation, firms would have access to less markets and less data as a result, which would undoubtedly lessen the rate of innovation.

## Scenario 3

### Stagnant Data Island

UK with full access to the Digital Single Market, but limited business ability to influence the regulatory regime.

The third scenario is named, “Stagnant Data Island” given the trade-off incurred to gain access to the Digital Single Market to the detriment of business’ ability to influence regulatory policy.

#### Opportunities

Three main opportunities would be borne out of this regime. Firstly, the UK would have a greater impetus to access other markets and engage with emerging economies. Secondly, we would most likely see a rise in privacy enhancing technologies. Thirdly, there would be considerable room for the UK to emerge as a personal data safe haven for other non-EU countries, whereby the UK could act as a personal data deposit.

#### Risks

However, “Stagnant Data Island” would present more risks than opportunities. First and foremost, the UK would be at risk of becoming less competitive than other countries, as it would be

forced to relinquish our favourable conditions for data innovation. Consequently, those with impressive data skills would be encouraged to go elsewhere and a brain drain would no doubt occur over time. This would be further encouraged by the fact that data would be prevented from being taken out of the UK to a less liberal regime.

## Scenario 4

### Enchanted Data Garden

UK with full access to the Digital Single Market, while businesses simultaneously influence the data legislative agenda. Our fourth scenario is called “Enchanted Data Garden” in reference to the abundant possibilities of data innovation and blossoming of UK data-intensive business, if the UK obtains full access to the Digital Single Market with businesses simultaneously being able to influence data protection legislation.

#### Opportunities

In this scenario, the opportunities for the UK data economy exceed the risks. Businesses would have increased ability to innovate with data, as they had access to more data. The UK would be able to choose its own regulatory regime to suit both business interests and broader legislative landscape. In addition, the opportunities of free trade and market access would result in more solid international links. The UK would be positioned as a data hub between the US and EU.

#### Risks

However, despite the many freedoms enjoyed in “Enchanted Data Garden,” there would still be at least three main risks to mitigate. Firstly, the predominance of business interests could result in decreased consumer trust. Secondly, this predominance could create a greater risk of data breach, as firms see themselves as not subject to strict regulatory regime. Thirdly, we could even see companies not investing in sufficient infrastructure to keep data safe.

Therefore, at its most beneficial, Brexit provides the opportunity for the UK to implement a new form of post-GDPR legislation inspired by the US model and to ensure that it is deemed ‘adequate’. Although the UK will not form part of the EU single market per se, it must strive to obtain access to the Digital Single Market by achieving adequacy status for data transfers. In doing so, the UK will have the opportunity to act as a ‘hub’ between Europe and the US. However, at its most detrimental, the UK could find itself with limited access to the Digital Single Market, while deemed inadequate by the European Commission with an almost identical GDPR with businesses holding no capital to influence the regime.

## Estimates for the UK data economy

Estimates for the data economy extend beyond the supply and demand of data to include the upstream and downstream value added arising from data markets and the wider benefits created through the wider multiplier effects through increased incomes and consumption. The IDC data breaks these down and estimates the contributions each make to the overall data economy. In the UK, in 2016 this is estimated to be €61.3 billion

Within our scenarios we can relate the two axes to components of the wider data economy:

- The forward indirect impacts are the benefits to the wider economy caused by the adoption of data products and services by “downstream” organisations. The utilisation of data by these organisations can potentially offer them productivity gains and a competitive advantage. The forward indirect impacts are represented by the vertical axis on our scenario matrix.
- The induced impacts are the economic activity caused by increases in employment and wages resulting from the growth of the data market (employees spending their earnings on consumer goods and services benefit the wider economy). The induced impacts relate to the horizontal axis on our matrix, this axis measures the level of access firms would have to the European Data Market.

Drawing on the published IDC scenario projections to 2020, the Challenge and High Growth, we have sought to estimate what the potential economic benefits are of our proposed regulation and access scenarios<sup>87</sup>.

- Starting from a position within Frozen Data Tundra, if we enable increased flexibility in data regulation but assume restrictions on market access the projected potential impacts are between €17 billion and €25 billion.
- Again starting from Frozen Data Tundra, if we apply a restriction to the flexibility in data regulation but assume complete access to the EU Digital Single Market the projected potential impacts are between €11 billion and €42 billion.
- Combining increased data flexibility with complete access to the EU Digital Single Market i.e. entering the Enchanted Data Garden, we estimate a projected potential impact of between €28 billion and €67 billion.

Therefore, it must strive to ensure that despite the traditional predominance of goods and services, data forms an integral element to the impending trade negotiations. As the government has stated, the UK will adopt GDPR, however it must ensure that the UK obtains access to the Digital Single Market, in conjunction with businesses gaining the ability to influence regulation. Though it is difficult to speculate whether the UK will be deemed adequate or not, it is important that if deemed inadequate, the UK is able to obtain special safeguards in the form of an improved Privacy Shield to suit UK interests. If the UK is able to come close to obtaining such an arrangement without compromising its position as a good destination for data and fast growing data economy, then there is no reason why it cannot become a ‘hub’ between the US and EU.

This report has already observed the similarities and differences in approach and application of data protection in the US and UK. Therefore, it is without question that the UK has a far more similar approach to legislation to the US than its European counterparts. Not only that, but there remains a cultural lineage bonding the two nations, despite disparate data protection standards in certain industries. Further, we have seen the ways in which the UK can learn from the US, in order to further garner the strength of the UK data economy. All of this, combined with the possibility of a US-UK trade deal, places the UK in an advantageous position to serve as a ‘hub.’ The main opportunity of the ‘hub’ scenario, would be the placing of the UK as the centre of activity, but more importantly the centre of data innovation. In contrast, the main risk would be in taking “Enchanted Garden” too far away from the EU model and, in doing so the EU could become less and less willing to honour special safeguards previously agreed upon (not dissimilar to criticism experienced by Privacy Shield).

<sup>87</sup> We have taken the IDC scenarios published estimates on the ‘forward indirect’ and ‘induced’ impacts. Where we consider there to be a constraint e.g. access to market we apply a weight of 0.5 on the project value of this effect. Where there is no constraint we apply a weight of 1. The estimates are weighted totals for combining ‘forward indirect’ and ‘induced’ for the 3 scenarios beyond the Frozen Data Tundra.



# Views from the roof



Insights from industry  
and policy makers

Many thanks to those consulted for this chapter, which included representatives from the Information Commissioner's Office (ICO), Department for Culture, Media and Sport (DCMS), the Department of International Trade, UKCloud, Meeco, Swiss Re, Ocado, Founders4Schools, CrowdEmotion, Squire Patton Boggs, the Royal Society and leading academics from Queen Mary University of London.

This chapter analyses Digital Catapult's findings from interviews with data businesses and industry experts. The discussions took the format of semi-structured interviews, which gave participants the freedom to express their views. Those interviewed were asked a series of questions, in order to assess the strengths, weaknesses, opportunities and threats surrounding data regulation post-Brexit. They were also asked for their thoughts regarding UK-US and EU-US legislation more broadly. These discussions provided insight into the five considerations Digital Catapult is making for further inquiry, and supported the ultimate aim of tracing the best possible outcome for the UK data economy in the final chapter.

## UK data economy strengths

The interviewees identified several strengths of the UK data economy related to both the future implementation of GDPR and Brexit. Firstly, there is a broad recognition by policymakers and business leaders of the necessity for a broad blueprint in data regulation. The extraterritorial effect of GDPR ensures that this blueprint will be felt well beyond Europe, even reaching US companies handling EU personal information.<sup>88</sup> Thus despite any weaknesses in the intricacies of the regulation, GDPR will be internationally recognised as a legitimate regulatory template. Even if the UK is granted sufficient freedom to let business determine legislation, the GDPR's international acceptance will be difficult to overcome. Secondly, our interviewees frequently referred to the UK's professionalism and competitiveness in data security as an important reason for setting up a business in the UK. Such a reputation provides a welcome environment for technological innovation. In fact, the UK is widely regarded as the best country to start a business, due to its low start-up costs coupled with a favourable climate for entrepreneurs.<sup>89</sup> In 2015, the Legatum Institute's Prosperity Report deemed the UK the third lowest cost place in the world to start a business, coming in with far greater business prospects than the US or Germany.<sup>90</sup> Along with France, the UK is the most ambitious and successful in data analytics. This coupled with London holding four times as many start-ups as the next best city for data, cements the prevailing view of it as a good destination for data. Thirdly, another of GDPR's strengths, lies in its ability to harmonise across divergent sectors within Europe. Consistency promotes business security and in turn can increase the capabilities of data more broadly. Finally, the GDPR comes at a time when the profile of privacy has been raised into the public conscience. There is a broad recognition that ultimately such a precise framework was needed, in order to provide more



clarity for business. The Data Protection Act 1998 is long outdated, just as European counterparts' legislation no longer suffices to guarantee safeguards for personal data. This is made evident as businesses have for a long time acknowledged the importance of expanding resources in the privacy arena by closely monitoring their use of personal data.

## UK data economy weaknesses

However, despite the many innovative features within GDPR, Digital Catapult encountered several concerns regarding the future of the UK data economy post-Brexit and the corresponding regulatory regime. After the referendum vote, businesses initially wondered whether they would have to implement GDPR at all. Firstly, skills generally form a recurring fear for data companies, as there continues to be a lack of sufficiently skilled labour. Brexit has exacerbated this weakness in the UK data economy, which has recently become more prominent. Nesta published a report in 2015, stating that data-driven companies are struggling to find suitable talent.<sup>91</sup> They found that the

88 Willey Rein LLP, "EU Finalizes General Data Protection Regulation: Implications for U.S. Businesses." January 2016. [http://www.wileyrein.com/newsroom-newsletters-item-EU\\_Finalizes\\_General\\_Data\\_Protection\\_Regulation.html](http://www.wileyrein.com/newsroom-newsletters-item-EU_Finalizes_General_Data_Protection_Regulation.html)

89 Giles Wilkes, "Low Costs Make UK Best Place in EU for Business Start-Ups." November 2015. <https://www.ft.com/content/29798670-80a9-11e5-a01c-8650859a4767>

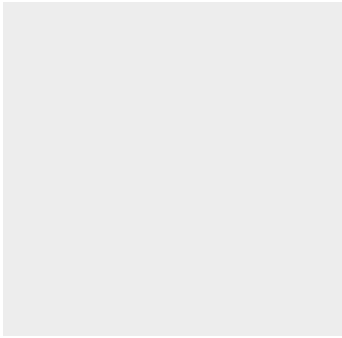
90 Maltby Harriet, "2015 UK Prosperity Report," Legatum Institute, November 2015. <http://www.li.com/activities/publications/2015-uk-prosperity-report>.

91 Nesta, Analytic Britain: Securing the Right Skill for the Data-Driven Economy. London: Nesta, 2015. 2. [https://www.nesta.org.uk/sites/default/files/analytic\\_britain.pdf](https://www.nesta.org.uk/sites/default/files/analytic_britain.pdf), 2.

issue lies in finding people who combine technical skills, analytics, industry knowledge and the business sense and soft skills to turn data into value.<sup>92</sup> The UK is faced with the dilemma of having the perfect conditions for data innovation, without the skills to garner it. Technology is developing at a quicker rate than the number of skills required to take advantage of it. Further, such concerns will only increase given the uncertainties surrounding freedom of movement post-Brexit. Secondly, there are several perceived injustices in both upcoming legislative changes and global perceptions of data regulation. As we have seen, the burden of regulation on US businesses is far lower than those in the UK given the increased freedom to form legislation in this sphere. Similarly, the burden of GDPR is far greater on smaller businesses, as they have far more to reformulate and create the conditions successful implementation of GDPR. This is further highlighted by the fact that several smaller businesses have begun to think about GDPR, but very few have made moves to ensure smooth implementation by 2018. This reiterates the increased burden on SMEs to implement GDPR, which are possibly hindering the capacity of the UK data economy for innovation. Such a disparity creates injustices within the UK data economy. Finally, and perhaps most importantly are several weaknesses identified by businesses assessing GDPR. Many businesses have found that legal basis for processing and consent are not well moulded to the UK system of law, while the terminology is impenetrable and makes it difficult to find the best way to comply.

### Opportunities for the UK from Brexit and GDPR

Despite several of the weaknesses listed, there are several opportunities borne out of the uncertainties. Firstly, the attempt at harmonisation across the single market, enables digital businesses to scale more easily and faster, thus enhancing their ability to compete and innovate on an internationally competitive level. Secondly, such an attempt raises the bar for privacy in the UK and elsewhere, as it is effectively a broad acknowledgement of the importance in developing the privacy sphere. Together with Brexit, the UK is presented with the opportunity to sample this new regulatory regime and then simplify it to better boost the data economy. The UK is in a position to develop a system that is at the very least as thorough and consumer-focused as GDPR, while simultaneously being simpler and therefore easier and less-costly for businesses to implement. Being able to sample this legislation prior to the UK's exit from the European Union, will undoubtedly place the UK in a unique position to tweak and then optimise the regulation. Thirdly, as discussed in Chapter 1, bilateral agreements with other countries such as the US



will be more likely outside of the European Union. Business leaders are cognizant of the opportunity that may present in the near future. However, many of them, especially those leading small businesses, are focused on the ramifications of Brexit for their opportunities for expansion into the Digital Single Market. Finally, GDPR provides the opportunity for increased efficiency once implemented. Businesses will eventually see the benefits of data minimisation, which will save money and time. That is, by keeping exclusively, the amount of data that is needed for the amount of time needed, efficiency will inevitably be increased. This coupled with the increased use of automation, will add value as GDPR forces companies to know where their clients' data is at any given moment.

### Threats to the UK from Brexit and GDPR

Such opportunities are not without threats, many of which could severely harm the UK data economy. Firstly, there are substantial risks regarding resources. It is difficult to predict whether DPAs will be sufficiently equipped to deal with the volume of cases once GDPR comes into effect. By the same token, many smaller businesses may not have the legal resources to comply and will face a greater threat of consecrating resources to comply to the detriment of revenues. Secondly, uncertainties surrounding terminology increase the threat of compliance. As we have seen, some of the language used throughout the GDPR obscures more than it illuminates. There is a severe risk of both businesses and the ICO being unsure of what non-compliance looks like. Thirdly, inadequacy presents a serious threat to the UK data economy and there is no way of understanding what such risks would entail until negotiations have begun. Fourth, several businesses acknowledged the serious risks regarding localisation of data. The uncertainties around GDPR make it difficult for businesses to know whether they should even store data in Europe anymore, given the possibilities that there may be barriers to do so in the future. Finally, the sheer costs of a breach under GDPR would risk sinking a smaller business far more than a larger one.

<sup>92</sup> Ibid, 6.

## Standardisation

One common theme addressed by the interviewees to this project, was to bridge the gap between regulatory reform and technological innovation. Interviewees suggested that the development of standards for data privacy could play a useful role in this environment, providing a mechanism of self-regulation within the existing legal framework.

There are a combination of factors responsible for the gap between new technologies and regulation. These are primarily i) the increasingly rapid pace of technological progress, which raises the policy workload required for a proper technical understanding of a new technology, in order for it to be effectively regulated; ii) the need for multiple stakeholders to have involvement during the design of the legislation, which often involves business, consumer and other groups, and is necessary for policy-makers to be able to assess the social and economic impact a new regulation might have; iii) and finally the need for feedback, scrutiny and approval by the various political institutions involved in the policy making process. Digital Catapult believes that compromising any of the above for the sake of a “more up-to-date” data regulatory framework engenders significant problems both for the digital industry as well as for the general public.

Two findings from the research supported this conclusion. The first is the apparent lack of agile technology-related legislation in relation to data privacy. The second is that it could be fairly argued that, despite their time consuming attributes, greater technical understanding, stakeholder involvement and political scrutiny are desirable goals for better regulation but could equally be achieved by the development of new standards, either industry-wide or in specific sectors.

It is important to note that standardisation is not suggested as a replacement for legislation, rather it is envisaged as an agility-enhancing precursor to regulation and/or a complement to it. Figures 4 and 5 present a diagrammatical representation of the relationship between self-regulation, co-regulation and legal regulation (which is the least agile but most thorough of the three). The self-regulation level involves the design, development and release of new privacy standards agreed upon by the industry members. The co-regulation level involves privacy standards mandated by the privacy regulator. In this case the regulator formally entrusts industry members to make privacy arrangements on its behalf, given that these are deemed to be sufficient by it after completion. The final level is that of formal regulation, where a privacy regulator enforces relevant legal arrangements following stakeholder involvement and political approval.

Under the GDPR (Article 25) ‘data protection by design and by default’ will be a legal requirement but essentially supports the idea that firms that avoid significant regulatory headaches by designing their products and services with privacy regulation in mind. The legislation does not provide sufficient detail as to how this should be interpreted, according to many firms interviewed for this study. Standards can help firms to implement such themes which are codified in the legislation, into a set of clearly understandable and implementable business processes through industry-specific self-regulation.

Figure 5: Agility of data protection regulation under the three main levels of stakeholder involvement in policy-making.

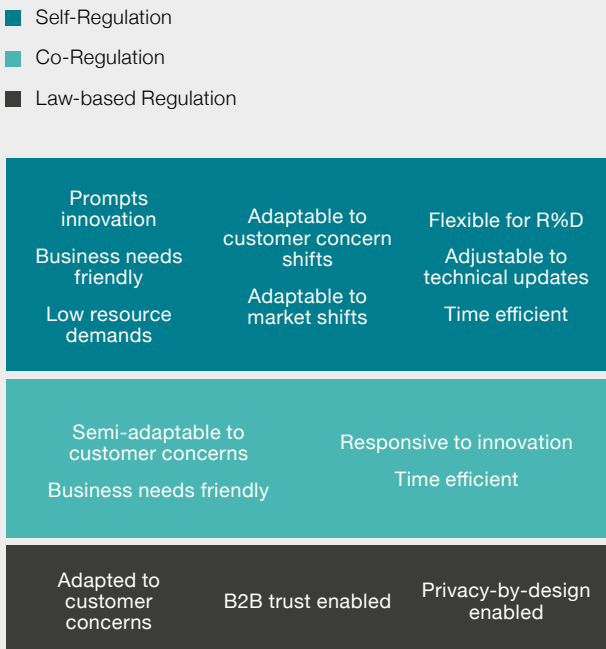
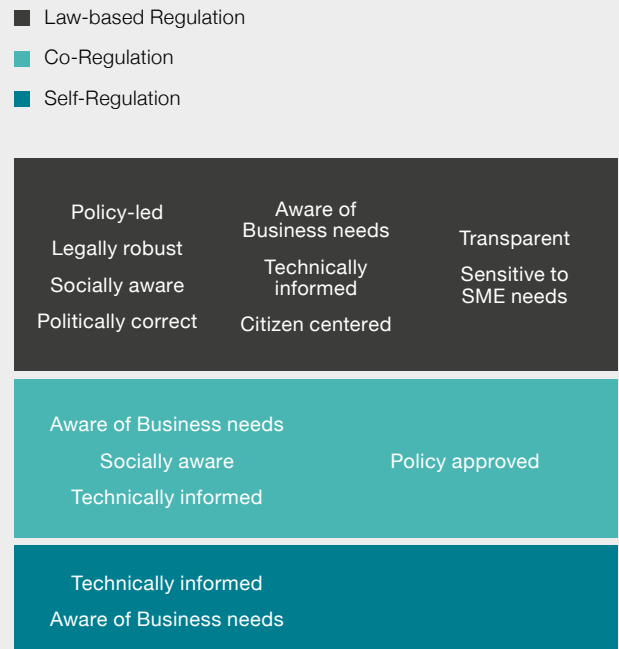


Figure 6: Thoroughness of data protection regulation under the three main levels of stakeholder involvement in policy-making.



Source: Digital Catapult Analysis

The second reason why this report recommends the introduction of privacy self-regulatory standards, is their potential for enhancing the UK-US post-Brexit trading relations, particularly with regards to data. As tariffs on data products and services are literally or virtually non-existent, any compromise in terms of removing data-trade barriers will most likely focus on regulation. It is important to ensure that there is sufficient regulatory homogeneity between the two countries in order for UK data businesses to be able to enter the US data market without facing deterring barriers and vice-versa. Hence, an industry level harmonisation would enable data businesses in both countries to expand more easily by lowering the cost and time of market entrance. As explained above, there is legal and enforcement incompatibility between the US and UK privacy regulation approaches. In addition, there is the issue of the sectoral and geographic segregation of privacy practices in the US (see chapter 2). These difficulties could be ameliorated by privacy self-regulation arrangements, as these will partly bridge existing differences. By enabling self-regulatory standards on the UK level, British data businesses will then be able to either coordinate or further co-develop their privacy practices

with their US industry counterparts. This would allow them to partly circumvent the rather impossible task of convincing US businesses and legislators to support large scale regulatory harmonisation amongst different sectors and states just for the sake of easier Anglo-American data trade.

In addition, even though the US has spearheaded industry-based standardisations, the EU has shown greater interest in exploring the possibility of a formalised arrangement for the introduction of 'alternative methods of regulation'.<sup>93</sup> Currently the European Data Protection Supervisor Board is discussing the creation of a privacy certification program. Given this, in combination with the fact that the ICO (UK) and FTC (US) are considering the development and endorsement of such standards as well, Digital Catapult argues that it is viable for them to become accepted as a precursory regulatory frameworks for data trade amongst developed economies.<sup>94</sup> This is especially for new technology related data, where regulatory and trade arrangements do not respond quickly to practical business needs and activities.

93 European Commission, Council and Parliament "Interinstitutional Agreement On Better Law-Making", Official Journal of the European Union, 2003/C, 321/01, (2003), "Community of Practice (CoP) for Better Self- and Co-regulation", Communications Networks, Content & Technology Directorate-General, June 3, (2014).

94 Federal Trade Commission, "Cross-Device Tracking", January 2017.



# Conclusions

Considerations for industry  
and policy makers



The final chapter of this report combines the primary and secondary research to offer some considerations for further discussion, inquiry, research and policy-making. Digital Catapult recommends that data flows and data markets form part of EU-UK trade negotiations, while simultaneously conditions around an attractive UK-US trade deal should be explored. Digital Catapult's findings also suggest that policy improvements in the context of localisation, simplification and certification could reduce the risks to data market growth as a result of Brexit and further stimulate the growth of the UK data economy.

### **Consideration 1** **Ensure that data flows, data markets and the wider data economy are taken into consideration in any UK-EU trade deal**

As mentioned previously, trade negotiations focus primarily on tangible goods and services and less so on intangibles. However, throughout this report the importance of data has been demonstrated for the world and for the continued growth of the UK data economy. Data's rise in importance highlights the necessity for policymakers to ensure that data markets and data flows are taken into account in the upcoming UK trade deal.

However, Digital Catapult fears that despite data's importance, discussion of it will not form an integral part in Brexit negotiations. There are three reasons for this. Firstly, data transfers are potentially not a salient enough topic for negotiations. Secondly, it may not be advantageous for British negotiators to tackle these considerations during negotiations. Thirdly, data trade would inevitably result in a "rational trade-off." These three reasons for ignoring any mention of data during negotiations are further exacerbated by the continuing level of uncertainty surrounding the UK's exit from the EU.

Digital Catapult argues that there are two crucial reasons that should deter British negotiators from ignoring data during negotiations. Firstly, while the UK may not have the same access to the single market, it is even more important to ensure that data flows between the UK and EU are unbounded as far as possible. At most this should be facilitated by the UK obtaining adequacy, but at the very least by the creation of a special safeguard not dissimilar to the Privacy Shield, despite its faults. Secondly, the potential for data to grow the British economy in the long-term is unquestionable. As we have seen, the UK data economy is currently the second largest in the EU, there are more data companies in the UK than anywhere else in Europe, the most data revenue and ICT spending. The continued predominance of the UK economy is dependent on data being a component of Brexit negotiations; data should be ignored at the peril of the economy.

### **Consideration 2** **Explore the conditions around an attractive UK-US trade deal which positions the UK as a data hub**

This report has demonstrated the opportunities and risks surrounding the UK functioning as a 'hub,' both the centre of innovation without compromising on British legislative tradition, while serving as a halfway-point between the EU and the US. Further, it has outlined the similarities and differences in approach and application of data protection in the UK and US. Given both countries' cultural similarities and the similarities of the UK and US legislative approaches compared to their European counterparts, this opportunity cannot be ignored.

Obtaining the 'hub' scenario would largely depend on exploration of the conditions around an attractive UK-US deal, while simultaneously ensuring that the UK is deemed 'adequate' in terms of its data privacy legislation, or operates on a Privacy Shield-like basis. Therefore, standards consistent with GDPR would be necessary. But equally important, would be obtaining the flexibility of the US regime, which would enable the UK to add value to US businesses wanting the free flow of data between the US and Europe via the UK.

### **Consideration 3** **Simplify UK data privacy regulation in comparison to GDPR**

Both regulators and businesses have mentioned a definite need for greater clarity in the GDPR, to which the UK will be subject in 2018, although without the freedom to influence its further development once the UK leaves the EU. Lack of clarity could lead to an increased abuse of the regulatory regime, as lawyers and business people interpret terminology in a way that suits their companies' interests. Digital Catapult's recommendation is to implement a version of GDPR more well-suited to the traditional UK system of law, while providing ample definitions of key terms. Far from advocating for a watered-down version of GDPR, Digital Catapult recommends a simplification to provide more clarity. It should be noted that given the territorial extent of GDPR, simplification whilst maintaining consistency would enable UK businesses to more easily comply whilst building the conditions for the UK data 'hub' discussed previously.

Simplification of GDPR would be beneficial to the UK data economy for three reasons. Firstly, as observed, the UK has a contrasting legislative system to its continental European counterparts with a system built on common law in addition to statute. However, there are many grey areas surrounding interpretation and enforcement of GDPR, which would be undertaken by the EU, therefore clearer insight as to how this will be achieved would provide much clarity. Secondly, as mentioned in the second chapter, simplification would be needed to define key terms, as and how they relate to the UK. Data portability in particular has not been clearly explained as it relates to the UK and there is no clear indication of its enforceability. Thirdly, there needs to be clearer definition of certain elements of GDPR, in order to make it easier for companies to understand when they are in breach in this new regime.

Therefore, Digital Catapult advocates simplifying the UK's regulatory regime, so that the UK can be considered adequate by the EU, while ensuring that the new data protection regime supports innovation in the growing data economy. It must be ensured that implementing GDPR does not leave the UK hostage to fortune in implementing legislation in which it no longer has a say in its development. Digital Catapult believes it is possible to implement legislation which provides the highest levels of privacy protection for citizens, whilst simultaneously promulgating a regime which is flexible to data flows, data transfers and which stimulates data innovation.

There is a lack of relevant studies which provide a monetary evaluation of the potential benefits of simplification, although some do exist.<sup>95</sup> In those studies the benefits of simplification were found to consist of a mixture of savings on: legal costs, public compliance costs, information acquisition costs and decision costs.<sup>96</sup> The weight of each of these factors varies depending on how the complexity of a policy is dealt with in terms of learning practices, perceptions, social effects, memory, personality cognition, emotions and motivation.<sup>97</sup> A 2014 study commissioned by the Business Taskforce of the UK Government puts the expected cost of GDPR compliance for small businesses to be up to £290 million<sup>98</sup>. It is Digital Catapult's view that a substantial proportion of this is related to unnecessary complexity that could be simplified.

## Consideration 4 Put in place measures to avoid localisation of data businesses to the UK

Localisation of data businesses to the UK is a significant threat for the UK post-Brexit. As noted previously (p.g. 42) localisation refers to the requirement that a firm maintains its data (and hence related facilities and personnel) in the market, country and regulatory space in which it operates. Several interviewees raised concerns about what the localisation risks would be post-Brexit, which highlights the extent to which more guidance is needed from policy makers. Interviewees mentioned the possibility of an increase in data storage costs and concerns about possible disruption of their EU expansion plans. Some interviewees stated that localisation might offer incentives for the creation of more UK-based storage facilities, which they in turn sighted as potentially beneficial in terms of reducing the latency of their services; but this was not a widespread view.

The extent and the overall cost of localisation will vary according to the arrangements made between the UK and the EU regarding data transfers. The European Centre for International Political Economy in a 2014 study estimated that the total economic impact of localisation for the EU as a whole could be a 0.8% reduction in GDP and a 1% reduction in total service exports.<sup>99</sup> The facts that the data economy is increasingly becoming an even larger part of the UK economic activity, and that the data sector is proportionally more developed in the UK than the average EU member, indicate that the above estimates will be even larger for the case of a post-Brexit Britain. Digital Catapult estimates that the potential cost of a post-Brexit total localisation of the UK will be a 1.2% reduction of the UKGDP or an annual loss of £22.5 billion.<sup>100</sup> The most defining factors for the extensivity of localisation would most likely be those of adequacy and a successful UK-EU data protection arrangement (both of which have been explored in Chapter 3). Digital Catapult recommends that policy-makers, business leaders and negotiators pay attention to these issues and to avoid any actions or decisions that may contribute to the localisation of UK data businesses.

95 Kahneman, Daniel. "A perspective on judgment and choice: mapping bounded rationality." *American psychologist* 58, no. 9 (2003): 697; Williamson, Oliver E. "The economics of governance." *The American Economic Review* 95, no. 2 (2005): 1-18; Simon, Herbert A. "A behavioral model of rational choice." *The quarterly journal of economics* 69, no. 1 (1955): 99-118.

96 Schuck, Peter H. "Legal complexity: some causes, consequences, and cures." *Duke Law Journal* 42, no. 1 (1992): 1-52.

97 Wisdom Services, "Regulation Complexity And The Costs Of Governance", *Corporate Governance and Business*, 2017. <https://www.wisdomjobs.com/e-university/corporate-governance-and-business-ethics-tutorial-354/complex-regulation-11026.html>

98 Business Taskforce, "Cut EU Red Tape: Report from the Business Taskforce." London: HMG (2014). <https://www.gov.uk/government/publications/cut-eu-red-tape-report-from-the-business-taskforce/cut-eu-red-tape-report-from-the-business-taskforce>

99 United States International Trade Commission (USITC) (2014), *Digital Trade in the U.S. and Global Economies*, Part 2; Bauer, Lee-Makiyama, van der Marel, and Verschelde (2014), *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE.

100 Post-Brexit GDP estimate has been based on IMF (2016) GDP projections for 2020. IMF Data, 2017. <http://www.imf.org/en/Data>

## Consideration 5 Use industry-wide and sector-specific data privacy standards as an alternative form of regulation

As previously discussed, Digital Catapult believes the introduction of industry-wide self-regulation and standards for data protection would undoubtedly benefit the UK data economy, and help to bridge the gap between regulatory reform and technological innovation. Instead of compromising the robustness of policy by pushing the speed of the policy-making process to match that of new IT developments, it would be beneficial to find an alternative methods of ensuring that data protection practices remain technologically contemporaneous. The need for such arrangements has also been expressed by various governmental privacy bodies, both in the Europe as well as the US.

In addition, in a joint 2015 study on 'The Economic Contribution of Standards to the UK Economy', an analysis contacted by the Centre of Economics and Business Research (CEBR) and a survey contacted by the British Standards Institution (BIS), suggest that, in the ICT related sectors, standardisation could result in a 2.8% increase in annual turnover and a 3.1% in exports.<sup>101</sup> Combining these with the Digital Catapult analysis of the UK data economy, Digital Catapult estimates that the adoption of industry level privacy standards in the post-Brexit UK, could yield an extra £430 million in annual revenue for data businesses, whilst the value of data-related service exports to the US could increase by £810 million. Therefore the total impact of standardisation on the UK data economy could exceed £1.2 billion in additional value created annually.

## Support for the use of standards in data privacy regulation

A recent report by the UK Information Commissioner's Office (ICO) proposes a series of 'compliance tools' that could help address data protection issues raised by the introduction of new technologies, specifically Big Data, Artificial Intelligence and Machine Learning. In this report the ICO does not prescribe the introduction of law-based regulation, but rather a combination of certification schemes, development of ethical frameworks, industry standardisation and other measures.<sup>102</sup> Similar attitudes towards self-regulation, and its agility enhancing benefits, have also been expressed by members of the Federal Trade Commission (FTC) in the US. Maureen Ohlhausen, current acting head of the Federal Trade Commission, has openly favoured self-regulation with regards to data protection of the emerging IoT device market.<sup>103</sup>

101 Hogan Oliver, Sheehy Colm and Jayasuriya Rajini. The Economic Contribution of Standards to the UK Economy, Centre of Economics and Business Research (CEBR) British Standards Institution (BIS), June 2015. <https://www.bsigroup.com/LocalFiles/en-GB/standards/BSI-The-Economic-Contribution-of-Standards-to-the-UK-Economy-UK-EN.pdf>, 90.

102 Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection", January 31, 2017. <https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/>

103 Thielman Sam, "Acting Federal Trade Commission head: internet of things should self-regulate", The Guardian, March 15, 2017. <https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation>

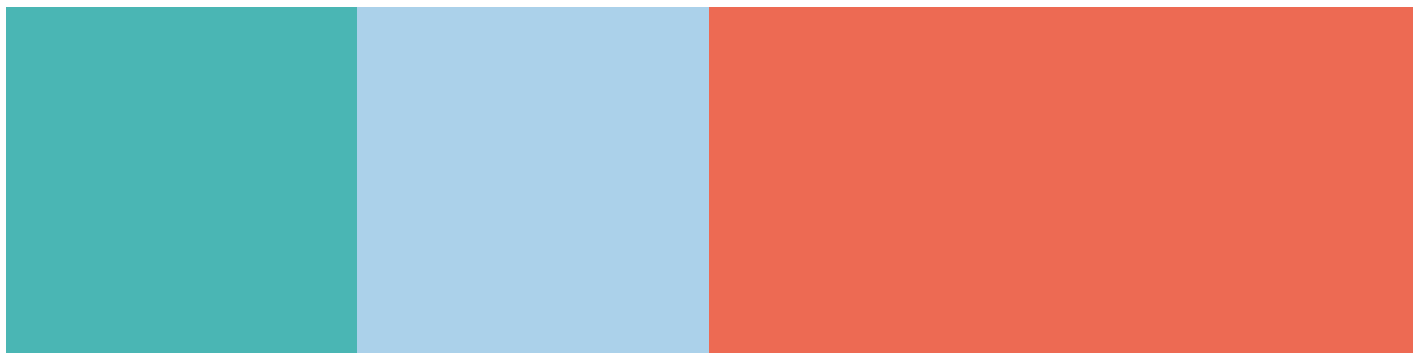
## Conclusion

The UK's very sizeable data economy and position outside of the EU places us in a unique position. The level of access to the Digital Single Market and amount of freedom for business to inform data regulation are essential to understanding the UK data economy post-Brexit. This report has outlined many of the possible opportunities and risks as they relate to these two flexible variables. The five recommendations for further research are an attempt to counteract the risks and take full advantage of the opportunities surrounding Brexit. Further inquiry into these five avenues would considerably benefit the UK data economy.

These five recommendations are an attempt for the UK to come as close as possible to the ideal scenario of "enchanted data garden," which would allow the UK full access to the Digital Single Market and for businesses to inform the direction of regulation in coming years. Digital Catapult believes the UK should ultimately be striving for a post-GDPR legislation inspired by the US model, while remaining adequate. If not deemed adequate, Digital Catapult advocate for similar special safeguards akin to Privacy Shield, but which maintain the thrust of privacy policy which has for so long maintained. If this regulatory regime can be achieved, the UK will have created the conditions to act as a data 'hub' between the US and Europe. Therefore, data must not be ignored during negotiations, a favourable bilateral agreement for the US and UK must be further explored, the UK must strive to simplify GDPR to better suit its institutions, the means of mitigating localisation risks must be found and self-certification schemes to bridge the gap between technology development and regulatory policy should be explored.

Technology and innovation will continue to develop at a much quicker rate than the development of regulatory reform. Such an imbalance creates an environment where ethical use of data becomes all the more important. Therefore, frameworks such as GDPR are more crucial than ever, in order to sufficiently secure citizens' personal privacy. However, some elements of this legislation are not well suited to British institutions. Both the interviews conducted and the statistical evidence consulted maintain that the UK will remain a competitive data economy even with the uncertainties surrounding Brexit.

Implementation of Digital Catapult's five recommendations could bolster the UK's economic potential with respect to data markets and the wider data economy and in doing so allow it to maintain its position as a premier destination for data in the post-Brexit world. Overall, the estimated total savings, efficiency gains and value created from implementing these recommendations could amount to as little as €8.6 billion<sup>104</sup> or as much as €43 billion, based on an estimate of 10% to 50% of the difference between the baseline scenario and the high-growth scenario of the size of UK data economy in 2020 calculated by IDC/ European Commission. This is equivalent to as much as 1.3% of post-Brexit GDP<sup>105</sup>. However, the equivalent risk could be as much as €4.8 Billion, based on 50% of the difference between the challenge scenario and baseline scenario, bearing in mind that the risks could have broader effects on the whole data economy<sup>106</sup>.



<sup>104</sup> Based on 10%-50% of the difference between the baseline and high growth data economy scenarios in 2020 calculated by IDC/ European Commission in The European Data Market Final Report: Study Dataset, <http://www.datalandscape.eu/study-reports>

<sup>105</sup> GDP in 2020 estimated to be €3,262 Billion in the high-growth scenario calculated by IDC/ the European Commission in The European Data Market Final Report: Study Dataset.

<sup>106</sup> *Ibid.*



# Bibliography

## A

95/ 46/ EC (General Data Protection Regulation).” Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/ 46/ EC (*gen. n.p.*, Accessed November 28th 2016. [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)).

Aaronson, Susan. “Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate Over Cross-Border Data Flows, Human Rights, And National Security”. *World Trade Review* 14, no. 04 (2015).

Andrews Natalie and Schlesinger M. Jacob “Senate Confirms Robert Lighthizer as Trump’s US Trade Representative’, *Wall Street Journal* (2017). Accessed 20 May 2017 <https://www.wsj.com/articles/senate-confirms-robert-lighthizer-as-trumps-u-s-trade-representative-1494529048>.

Asinari, María Verónica Perez. “The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?.” 18th BILETA Conference: Controlling Information in the Online Environment (2003).

## B

Bauer, Lee-Makiyama, van der Marel, and Verschelde (2014), *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE.

Bennett, Steven C. “The ‘right to be forgotten’: Reconciling EU and US Perspectives.” *Berkeley Journal of International Law* 30 (2016).

Bignami, Francesca and Giorgio Resta. “Transatlantic Privacy Regulation: Conflict and Cooperation.” Vol. 78. Washington DC: GW Law Faculty Publications (2015).

Bird & Bird All Rights Reserved. *Guide to the General Data Protection Regulation*. London: Bird and Bird LLP, 2016. Accessed December 9th 2016 <https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>.

Biscop Daniel, “Donald Trump: I’ll do a deal with Britain”. *The Times*, January 16, 2017. Accessed February 10, 2017. <https://www.thetimes.co.uk/edition/news/i-ll-do-a-deal-with-britain-6hl2hl73l>

Bloom, Jonty. “Reality Check: Can There Be a Quick UK-USA Trade Deal?” *BBC Business (BBC News)*, January 16, 2017. Accessed February 10th 2017. <http://www.bbc.co.uk/news/business-38639638>.

Bonneau, Joseph and Sören Preibusch, “The Privacy Jungle: On the Market for Data Protection in Social Networks.” Cambridge University Press (2009).

Bradford, Anu. “The Brussels Effect.” *Northwestern University School Law Review* (2012).

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* 3rd ed. Reading, MA: Perseus Books, 1999.

“Building the European Data Economy,” January 10, 2017. Accessed January 12, 2017, [http://europa.eu/rapid/press-release\\_MEMO-17-6\\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-6_en.htm).

Business Taskforce, “Cut EU Red Tape: Report from the Business Taskforce.” London: HMG (2014). Accessed 2 March 2017. <https://www.gov.uk/government/publications/cut-eu-red-tape-report-from-the-business-taskforce/cut-eu-red-tape-report-from-the-business-taskforce>

## C

Carey, Peter LL. M. *Data Protection: A Practical Guide to UK and EU Law*. 3rd ed. New York: Oxford University Press, 2008.

Carter, Jamie. *How to Handle the New US-EU Data Regulations*. (TechRadar), May 23, 2016. Accessed March 18th 2017 <http://www.techradar.com/news/internet/how-to-handle-the-new-us-eu-data-regulations-1320554>.

Cattaneo, Gabriella, Mike Glennon, Rosanna Lifonti, Giorgio Micheletti, Alys Woodward, Marianne Kolding, and David Osimo. *European Data Market Study, Second Interim Report: The Data Market in the World*. Luxembourg: IDC, 2016. <http://www.datalandscape.eu/study-reports>.

Cattaneo, Gabriella, Mike Glennon, Rosanna Lifonti, Giorgio Micheletti, Alys Woodward, Marianne Kolding, and David Osimo. *European Data Market Study, Second Interim Report: Citizens’ Reliance on Data*. Luxembourg: IDC, 2016. <http://www.datalandscape.eu/study-reports>.

Cattaneo, Gabriella, Mike Glennon, Rosanna Lifonti, Giorgio Micheletti, Alys Woodward, Marianne Kolding, and David Osimo. *European Data Market Study, Second Interim Report: Study: Methodology Report*. Luxembourg: IDC, 2016. <http://www.datalandscape.eu/study-reports>.

Cattaneo, Gabriella, Mike Glennon, Rosanna Lifonti, Giorgio Micheletti, Alys Woodward, Marianne Kolding, and David Osimo. *European Data Market Study, Second Interim Report: Study: Data Market and the Data Economy*. Luxembourg: IDC, 2016. <http://www.datalandscape.eu/study-reports>.

Carter, Jamie. How to Handle the New US-EU Data Regulations. (TechRadar), May 23, 2016. Accessed January 17th 2017 <http://www.techradar.com/news/internet/how-to-handle-the-new-us-eu-data-regulations-1320554>.

CMA, "The Commercial Use of Consumer Data", 2015. Accessed February 19th, 2017. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/435817/The\\_commercial\\_use\\_of\\_consumer\\_data.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf)

Cobb, Stephen. Data Privacy and Data Protection: US Law and Legislation. n.p.: CISSP, 2016. Accessed January 9th 2017 <http://www.welivesecurity.com/wp-content/uploads/2016/04/US-data-privacy-legislation-white-paper.pdf>.

Coffin David and Stamps James , "Digital Trade in the U.S. and Global Economies, Part 2", US Interntional Trade COmission, 2014. Accessed February 20, 2017. <https://www.usitc.gov/publications/332/pub4485.pdf>

Council of the European Union and European Parliament, 'General Data Protection Regulation/ Article 25: Data protection by design and by default' Official Journal of the European Union, Regulation 2016/679, Assented 27 April 2016.

Craig Richard, "The 'one stop shop" TaylorWessing, April 2016. Accessed January 17, 2017. <https://united-kingdom.taylorwessing.com/globaldatahub/article-the-one-stop-shop.html>.

## D

"Data Protection in the United States: Overview," Practical Law, 2016, accessed January 5, 2017, <http://uk.practicallaw.com/6-502-0467>.

De Bièvre, Dirk, and Andreas Dür. "Constituency interests and delegation in European and American trade policy." *Comparative Political Studies* 38.10 (2005): 1271-1296.

Department of Justice, Office of the Attorney General, "Judicial Redress Act of 2015; Attorney General Designations", Federal Register, January 23, 2017. Accessed February 5, 2017. <https://www.federalregister.gov/documents/2017/01/23/2017-01381/judicial-redress-act-of-2015-attorney-general-designations>

Dominiczak, Peter. "Theresa May and Donald Trump to Hold Talks on Trade Deal That Cuts Tariffs and Allows Workers to Move Between the US and UK." *The Telegraph* (The Telegraph), January 23, 2017. <http://www.telegraph.co.uk/news/2017/01/22/theresa-may-donald-trump-hold-talks-trade-deal-cuts-tariffs/>.

Donnan Shawn, "Trump's UK trade pledge: hurdles to a quick deal". *Financial Times*. January 16, 2017. Accessed February 11, 2017. <https://www.ft.com/content/378c2678-db9d-11e6-9d7c-be108f1c1dce>.

## E

Elliot Larry, "Brexit Britain is suddenly debating trade – but it's the wrong talking point", *The Guardian*, March 19, 2017. Accessed February 4 2017. <https://www.theguardian.com/business/economics-blog/2017/mar/19/brexit-britain-talking-trade-deal-eu-wrong-talking-point>.

"EU Finalizes General Data Protection Regulation: Implications for U.S. Businesses." January 2016. Accessed January 2, 2017. [http://www.wileyrein.com/newsroom-newsletters-item-EU\\_Finalizes\\_General\\_Data\\_Protection\\_Regulation.html](http://www.wileyrein.com/newsroom-newsletters-item-EU_Finalizes_General_Data_Protection_Regulation.html).

European Commission, Council and Parliament "Interinstitutional Agreement On Better Law-Making", Official Journal of the European Union, 2003/C, 321/01, (2003). [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003Q1231\(01\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003Q1231(01)&from=EN)

European Commission, "Community of Practice (CoP) for Better Self- and Co-regulation", Communications Networks, Content & Technology Directorate-General , June 3, (2014). Accessed March 13, 2017. [https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Conclusions%20from%20the%20Chair\\_0.pdf](https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Conclusions%20from%20the%20Chair_0.pdf).

European Commission, "A Digital Single Market Strategy for Europe", 2015. Accessed January 16, 2017. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>; <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN> .

European Commission, "The Digital Economy and Society Index", 2017. Accessed January 16, 2017. <https://ec.europa.eu/digital-single-market/desi#desi-scores-by-dimension>; <https://www.theguardian.com/technology/2015/may/06/eu-unveils-plans-digital-single-market-online-firms>.

European Commission, "e-Commerce Directive", 2015. Accessed January 17, 2017. <https://ec.europa.eu/digital-single-market/en/e-commerce-directive>.

European Commission, "Proposed Directive establishing the European Electronic Communications Code", 2015. Accessed January 17, 2017. <https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code>.

European Commission, "Building the European Data Economy." January 10, 2017. Accessed March 1, 2017. [http://europa.eu/rapid/press-release\\_MEMO-17-6\\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-6_en.htm).

European Commission, "Commission Decisions On The Adequacy Of The Protection Of Personal Data In Third Countries - European Commission", Ec.Europa.Eu, 2017, [http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).

European Commission, "Staff Working Document on the Free Flow of Data



and Emerging issues of the European Data Economy", 2017. Accessed January 20, 2017. <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>.

European Commission, "Communication on Building a European Data Economy", 2017. Accessed January 21, 2017. <https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>.

EuroStat Database, 2016. Accessed December 11, 2016. <http://ec.europa.eu/eurostat/data/database>.

## F

Federal Trade Commission, "Cross-Device Tracking", January 2017. Accessed March 20, 2017. [https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc\\_cross-device\\_tracking\\_report\\_1-23-17.pdf](https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf).

Frontier Economics, "The UK Digital Sectors After Brexit". London: 2017 TechUK. Accessed January 30, 2017. <http://www.frontier-economics.com/de/documents/2017/01/the-uk-digital-sectors-after-brexite.pdf>.

Foundation, Legatum Institute and All right reserved. "2015 UK Prosperity Report." November 2015. Accessed February 1, 2017. <http://www.li.com/activities/publications/2015-uk-prosperity-report>.

## G

Giles Wilkes, "Low Costs Make UK Best Place in EU for Business Start-Ups." November 2015. Accessed February 22nd 2017 <https://www.ft.com/content/29798670-80a9-11e5-a01c-8650859a4767>.

Global Open Data Index, "Place Overview," 2016. Accessed February 19th, 2017. <https://index.okfn.org/place/>.

## H

Hanke Jacob and Mucci Alberto, Theresa May's Brexit trade bluff, Politico, April 3, 2017. Accessed April 5, 2017. <http://www.politico.eu/article/theresa-may-brexite-trade-bluff-uk-economy-negotiation-eu/>.

Hart-Davis, Damon. "Spinning That Brexit Wheel: Regulation Lotto for Tech Startups." 2016. Accessed February 20, 2017. [http://www.theregister.co.uk/2016/09/06/regulation\\_lotto\\_for\\_tech\\_startups/](http://www.theregister.co.uk/2016/09/06/regulation_lotto_for_tech_startups/).

Hartzog, Woodrow and Daniel J. Solove. "The Scope and Potential of FTC Data Protection." George Washington University Law School 83, no. 6 (November 2015).

Hornung, Gerrit. "A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012." SCRIPTed 9, no. 1 (April 15, 2012): 64–81

ICO. "Taking Action - Data Protection." December 8, 2016. Accessed January 8, 2017. <https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/>.

## I

IDC, "European Data Market: Final Report." Accessed May 2, 2017. <http://www.datalandscape.eu/study-reports>.

IDC "Worldwide Black Book Pivot Table", 2016, IDC, (2016). Accessed February 13, 2017, <https://www.idc.com/getdoc.jsp?containerId=US41686816>.

IDC, Press Release: "Worldwide Big Data and Business Analytics Forecast to Reach \$187 billion in 2019." Accessed March 5, 2017. <https://www.idc.com/getdoc.jsp?containerId=prUS41306516>.

IMF Data Mapper, (2017). Accessed March 1, 2017. <http://www.imf.org/en/Data>.

Information Commissioner's Office, "The Guide to Data Protection", January 31, 2017. Accessed February 13, 2017. <https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/>.

Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection" March 1, 2017. Accessed March 7, 2017. <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

Inside Trade, "Official: White House position on TTIP up in the air until Lighthizer is confirmed", March, 2017. Accessed 26 March, 2017. <https://insidetrade.com/daily-news/official-white-house-position-ttip-air-until-lighthizer-confirmed>.

## J

Jolly, Ieuan and Loeb. "Data Protection in the United States: Overview." 2016. Accessed January 5, 2017. <http://uk.practicallaw.com/6-502-0467>.

## K

Khan, Mehreen. "UK Trade Deficit Hits £12.5bn in Brexit Month." Financial Times, 2016. Accessed 1st March 2017 <https://www.ft.com/content/0965cbd6-64d8-31b0-8cd2-a2697d28bd52>.



Koops, B. -J. "The Trouble with European Data Protection Law." *International Data Privacy Law* 4, no. 4 (October 8, 2014): 250–61. doi:10.1093/idpl/ipu023.

Korff, Douwe. "EU-US Umbrella Data Protection Agreement: Detailed Analysis by Douwe Korff." October 14, 2015. Accessed January 23, 2017. <https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/>.

Kuner, Christopher, "Reality and Illusion in EU Data Transfer Regulation Post Schrems." *German Law Journal* 14 (2016).

Kuner, Christopher, *The Internet and the Global Reach of EU Law* (February 1, 2017). Forthcoming in the *Collected Courses of the Academy of European Law* (Oxford University Press). Available at SSRN: <https://ssrn.com/abstract=2890930> or <http://dx.doi.org/10.2139/ssrn.2890930>.

## M

MacDonald, Diane A., and Christine M. Streatfeild. "Personal Data Privacy and the WTO." *Houston Journal of International Law*. 36 (2014): 625.

Mandel Michael, "Data Trade and Growth", 2014. Progressive Policy Institute. Accessed January 11, 2017. [http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel\\_Data-Trade-and-Growth.pdf](http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf).

Maltby Harriet, "2015 UK Prosperity Report," Legatum Institute, November 2015. Accessed February 1, 2017. <http://www.li.com/activities/publications/2015-uk-prosperity-report>.

McCarthy Kieren, "Trump signs 'no privacy for non-Americans' order – what does that mean for rest of us?", *The Register*, January 26, 2017. [https://www.theregister.co.uk/2017/01/26/trump\\_blows\\_up\\_transatlantic\\_privacy\\_shield/](https://www.theregister.co.uk/2017/01/26/trump_blows_up_transatlantic_privacy_shield/).

McKinsey Global Institute, "Digital Globalization: the New Era of Global Flows", 2016. Accessed January 12. <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>.

Meltzer, Joshua Paul. "The Internet, Cross-Border Data Flows and International Trade." *Asia & the Pacific Policy Studies* 2.1 (2015): 90-102.

Moore, Tyler, David Pym, and Christos Ioannidis, eds. *Economics of Information Security and Privacy*. New York: Springer-Verlag New York, 2010.

## N

Nathan, Max, Anna Rosso, Tom Gatten, Prash Majmudar, and Alex Mitchell. *Measuring the UK's Digital Economy with Big Data*. London: National Institute of Economic and Social Research, 2013.

Nesta. *Analytic Britain: Securing the Right Skill for the Data-Driven Economy*. London: Nesta, 2015. Accessed February 17th 2017. [https://www.nesta.org.uk/sites/default/files/analytic\\_britain.pdf](https://www.nesta.org.uk/sites/default/files/analytic_britain.pdf).

## O

OECD. *The Knowledge-Based Economy*. Paris: OECD, 1996. Accessed 19th March <https://www.oecd.org/sti/sci-tech/1913021.pdf>.

OECD Internet Economy Outlook 2012; Meltzer, Joshua Paul. "The Internet, Cross-Border Data Flows and International Trade." *Asia & the Pacific Policy Studies* 2.1 (2015): 90-102.

OECD. *The Knowledge-Based Economy*. Paris: OECD, 1996. Accessed 19th March <https://www.oecd.org/sti/sci-tech/1913021.pdf>.

OECD WTO UNCTAD, "Implications Of Global Value Chains For Trade, Investment, Development And Jobs", G20 Leaders Summit, St. Petersburg (2013).

"The 'one stop shop.'" April 2016. Accessed January 17, 2017. <https://united-kingdom.taylorwessing.com/globaldatahub/article-the-one-stop-shop.html>.

## P

Palmisano, Samuel J. "The globally integrated enterprise." *Foreign affairs* (2006): 127-136.

Preibusch, Soren. "The Value of Web Search Privacy." *IEEE Security & Privacy* 13, no. 5 (September 2015): 24–32. doi:10.1109/msp.2015.109.

Petersburg, Saint. "Implications of Global Value Chains For Trade, Investment, Development and Jobs." (2013).

Putnam, Robert D. "Diplomacy and domestic politics: the logic of two-level games." *International organisation* 42, no. 03 (1988): 427-460.

"Privacy, Identity & Online Security | Consumer Information". *Consumer.Ftc.Gov*, 2017. Accessed February 16, 2017. <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

## R

Raul, Alan Charles. "The Privacy, Data Protection and Cybersecurity Law Review." London: Law Business Research (2014).

## S

Shaffer, Gregory. "The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice." *European Law Journal* 5, no. 4 (December 1999): 419–37. doi:10.1111/1468-0386.00089.

Singer, Natasha. "Consumer Data Protection Laws, an Ocean Apart." *Technology* (The New York Times), February 2, 2013. Accessed December 19th 2016 [http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?\\_r=1&](http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?_r=1&).

"Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment", Ec.Europa.Eu, 2016. Accessed 13th March 2017 [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2016/20160203\\_statement\\_consequences\\_schrems\\_judgement\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf).

Stevens, Gina. "The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority." Congressional Research Service (2014).

Stupariu, Ioana. "Defining the Right to Be Forgotten: A Comparative Analysis Between the EU and the US." SSRN Electronic Journal. doi:10.2139/ssrn.2851362.

## T

Teshuva, Ariel. "Why Has the EU Made So Few Adequacy Determinations?" Washington DC: Lawfare, January 2 2017. Accessed January 17 2017. <https://www.lawfareblog.com/why-has-eu-made-so-few-adequacy-determinations>.

Thielman Sam, "Acting Federal Trade Commission head: internet of things should self-regulate", *The Guardian*, March 15, 2017. Accessed March 22, 2017. <https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation>.

Training, Further education and, Research and development, Broadband investment, UK economic growth, Department for Culture, Media & Sport, and The Rt Hon Karen Bradley. "Documents." March 1, 2017. Accessed March 1, 2017. <https://www.gov.uk/government/publications/uk-digital-strategy>.

Traynor Ian, "EU Unveils Plans to Set up Digital Single Market for Online Firms", *The Guardian*, May 6, 2015. Accessed January 17, 2017. <https://www.theguardian.com/technology/2015/may/06/eu-unveils-plans-digital-single-market-online-firms>.

## U

UK Government, "The United Kingdom's exit from and new partnership with the European Union" [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/589191/The\\_United\\_Kingdoms\\_exit\\_from\\_and\\_partnership\\_with\\_the\\_EU\\_Web.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589191/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf).

UK Government, "UK Digital Strategy", Department of Culture, Media and Sport, March 1, 2017. Accessed March 1, 2017, <https://www.gov.uk/government/publications/uk-digital-strategy>.

US Government, "KORUS FTA" Korea-United States Free Trade Agreement, Article 15.8, Electronic Commerce/Cross-Border Information Flows, 2012. Accessed January 14, 2017. [https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset\\_upload\\_file816\\_12714.pdf](https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf).

United States Senate, "Hearing on the Nomination of Robert E. Lighthizer to be United States Trade Representative", Committee on Finance, 2017. Accessed March 27, 2017. <http://g8fip1kplyr33r3krz5b97d1.wpengine.netdna-cdn.com/wp-content/uploads/2017/03/Lighthizer-QFR-FINAL.pdf>.

United States International Trade Commission (USITC) (2014), *Digital Trade in the U.S. and Global Economies*, Part 2

## V

Von Der Burchard, Hans, "Trump's pick for trade envoy open to continued EU trade talks", *Politico*, March 21, 2017. Accessed March 22, 2017. <http://www.politico.eu/article/trumps-pick-for-trade-envoy-open-to-continued-eu-trade-talks/>.

Voss and W Gregory. "Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later by W. Gregory Voss: SSRN." February 21, 2015. Accessed November 28, 2016. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2567624](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567624).

## W

Watts, Joe. "Donald Trump and Theresa May Agree Immediate Talks on Post-Brexit Trade Deal." *The Independent - UK Politics (Independent)*, January 28, 2017. <http://www.independent.co.uk/news/uk/politics/donald-trump-theresa-may-trade-deal-brexit-lunch-european-union-holding-hands-menu-card-a7550956.html>.

Weiss, Martin A and Kristin Archick. *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*. Washington DC: Congressional Research Service, 2016. <https://fas.org/sgp/crs/misc/R44257.pdf>.

Wiley Rein LLP, "EU Finalizes General Data Protection Regulation: Implications for U.S. Businesses." January 2016. *Accessed January 2, 2017*. [http://www.wileyrein.com/newsroom-newsletters-item-EU\\_Finalizes\\_General\\_Data\\_Protection\\_Regulation.html](http://www.wileyrein.com/newsroom-newsletters-item-EU_Finalizes_General_Data_Protection_Regulation.html).

White House. "Executive Order: Enhancing Public Safety in the Interior of the United States." Office of the Press Secretary, 2017. *Accessed February 5, 2017*. <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>.

"WTO | WTO Analytical Index: Guide to WTO Law and Practice - General Agreement On Trade in Services". *Wto.Org*, 2017. [https://www.wto.org/english/res\\_e/booksp\\_e/analytic\\_index\\_e/gats\\_02\\_e.htm](https://www.wto.org/english/res_e/booksp_e/analytic_index_e/gats_02_e.htm).

WTO, "General Agreement on Trade in Services", 1995. *Accessed January 12, 2017*. [https://www.wto.org/english/res\\_e/booksp\\_e/analytic\\_index\\_e/gats\\_02\\_e.htm](https://www.wto.org/english/res_e/booksp_e/analytic_index_e/gats_02_e.htm).

**CATAPULT**  
Digital

We work with  
**Innovate UK**

@digicatapult · #wheredigitalinnovationlives · digicatapult.org.uk