HMT Discussion Paper: The Economic Value of Data
Barclays Response

Barclays is a transatlantic consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. With over 325 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

Barclays welcomes the opportunity to engage with HM Treasury regarding the economic value of data in a modern digital economy. As a major UK financial institution with data at the heart of everything we do for our customers and clients, we are well placed to provide insights and expertise in this area.

We provide comments on a number of themes explored in the Discussion Paper. We hope these insights are valuable, and would of course be happy to discuss them further if helpful.

Index

1. Key Policy Recommendations
2. Introduction
3. The Value of Data for Consumers and Business
4. Artificial Intelligence
5. Enabling Safe Data Sharing to Create Economic Value
6. Data Privacy and Protection
7. Data and Digital Trade

Key Policy Recommendations

Value of Data for Consumers and Business

- Industry should be responsible for ensuring consumers understand their legal rights regarding the use of their data, and explain how they are being observed and safeguarded.

Artificial Intelligence

- Government should develop a framework of ethical guidelines for industry to adhere to when creating AI systems.
- Government should consider developing guidance or a liability framework for third party outsourcing of AI activities.
- Government should invest in AI education at schools and universities to ensure the UK has the right skills to lead going forward.
- Government should consider how automated decision making provisions under GDPR could be approached to enable AI and other technologies to deliver the most benefit.

Establishing Safe Data Sharing Frameworks

- Government should consider lessons learnt in the development of the Open Banking framework, when developing new data sharing frameworks.
- Government should explore extending the Open Banking framework beyond the CMA 9 to all banks.
- Government should consider the introduction of data sharing frameworks in other data-rich sectors, e.g. the tech sector.
- Government should facilitate the development of common standards for data portability, with standardised templates appropriate for each sector.
- Government should seek to maximise consumers' awareness of their data portability rights. Service providers should also be required to ensure consumers are aware of their rights and fully understand that they can request their personal data to share with other firms if they choose to.

Data Privacy and Protection

- Government should lead the development of global standards for data protection and interoperability between jurisdictions.
- Government should seek to achieve a data adequacy decision from the EU, as soon as possible.
- Government should review the liability framework for merchant data breaches to ensure that those who allow data losses bear the full costs of those data losses, including any costs of third parties that can be accurately associated to their data loss.

Data and Digital Trade

- Government should push back against any data localisation trends on the international stage and ensure an appropriate international framework exists for cross border data flows.

1. Introduction

The digital revolution is fundamentally changing the way in which businesses operate and the way users manage their lives. Almost all sectors are being impacted by digitisation to some extent, with financial services in particular being transformed. Indeed, over the next few years, almost all financial services will be conducted digitally as consumers and clients increasingly choose online digital offerings over traditional channels such as branches.

And as consumers increasingly engage digitally, they generate a data profile with their provider that develops over time. The volumes of data being generated are huge, and firms are only just starting to try and better understand it. However, advances in technology are increasingly able to help. The rise of artificial intelligence and 'big data' technologies is helping firms process and understand the enormous data sets they find themselves holding, allowing them to make more informed decisions and create greater value.

When consumer data can be understood and leveraged appropriately, it has the potential to have significant economic value, both for firms and consumers. For firms, data can provide unprecedented insights into their customers which can be used to tailor products and services appropriately. For consumers, rights and capabilities to share their personal data with third parties provide enormous potential for consumers to leverage their data and receive meaningful economic benefit. But with greater consumer control over their data, also comes greater data privacy risks to consider.

2. The Value of Data for Consumers and Business

As markets across the economy become increasingly digital, consumers are generating more and more data that is held by their service provider. This data can provide insights on the consumer that previously have been unavailable to firms, but have the potential to benefit both the consumer and the firm itself. These consumer insights are inherently valuable as they enable business to better understand their consumers and market place, while allowing consumers to benefit from more intelligent and consumer focused products and services. Furthermore, new data sharing capabilities are well positioned to create significant economic value as consumers are empowered to harness their data for their own benefit – see Section 4.

Increasing volumes of data are already changing how financial services firms operate and engage with their customers. For example:

- **Tailored Customer Service** – as consumers engage with firms on an ongoing basis, they continually develop a data profile that firms use to better understand their consumers and offer a differentiated service. For example, data showing a young person has received a student loan payment could enable the firm to classify them as a student and therefore offer an appropriate product such as a Student Current Account, with clear benefit to the consumer.

- Insurance also provides a clear example of data enabling value creation. Providers will assess a consumer's needs against their data profile to generate a price that reflects the cost of any service provision. Ultimately, the use of data leads to fairer, more efficient outcomes and effective risk management.

- **Vulnerable Customers** – financial services firms are increasingly using their consumers' data to provide more holistic support to their most vulnerable customers. Barclays has developed a 'Financial Stress Data Engine' that looks at a combination of data points, such as sustained overdraft usage and low levels of funds remaining after expenses, to identify potential vulnerability and limited resilience to a financial shock. When consumers are clearly identified as struggling, we are now able to proactively engage them to offer support and tools to help improve their financial health. Recent research suggests consumers support banks using their data to identify and support potentially vulnerable customers or customers clearly experiencing financial distress. The research was clear consumers prefer a *direct approach* from their bank when clearly experiencing financial distress, but a *softer, more indirect approach* if data indicates only potential signs of financial difficulty. While there is strong potential for banks to use consumer data to support vulnerable customers, it is important that firms build consumer understanding to alleviate any potential fears around transparency. Of course, it is important to ensure that any consumers identified as being vulnerable are not unfairly excluded or disadvantaged as a result.

- The FCA have recognized that often banks have a strong commercial incentive to assess a consumer's credit risk when taking lending decisions, but less incentive to assess the risk that that credit will negatively impact the consumer's broader personal financial situation. Therefore, on 1 November, the FCA clarified that the requirement to assess creditworthiness incorporates both the customer's ability to repay any credit, and their ability to meet the repayments without significantly impacting their financial situation. Barclays' existing creditworthiness assessments already reflect this clarification. This is a positive example of where consumers' data is currently being used for their benefit within the unsecured lending market.

Transparency and Consumer Understanding

While increasing volumes of data have the potential to create significant economic value, industry moves to use develop and deliver new and innovative products and services need to be carefully balanced with the need to protect consumers. As data becomes more valuable, firms will increasingly look to persuade consumers to provide their data in exchange for, or as part of, a service. Indeed, as is commonly highlighted, if services are provided for free, provision of data is often the price consumers pay in return for the service. It is important therefore that consumers understand what data they are providing to firms, and that firms are transparent as to what data they are requesting, how it will be collected, for what purpose(s) it will be used, and by whom. Ultimately, transparency is key to generating consumer trust in the collection and use of their data by business.

Furthermore, as processing of consumer data becomes increasingly automated, it will become more difficult for consumers to provide informed consent (if required) or even know whether their data is being processed in the first place. While data protection rules have long required firms to explain to customers how they will use their data, and GDPR has enhanced those rules further, industry should be responsible for ensuring consumers know their legal rights regarding their data, and explain how they are being observed and safeguarded.

Consumer understanding is especially important in the context of data sharing. As consumer data sharing becomes common place, and consumers are increasingly encouraged to share their data with third parties, it is vital they have full understanding of how their data is being used, any potential risks associated with sharing their data, and the steps they can take to avoid any potentially negative consequences. There is also a responsibility of firms to be crystal clear when they would be accessing consumer data held elsewhere, to ensure consumers can make well informed decisions and ensure they only share their data knowingly.

Barclays has made deliberate efforts to raise public awareness around and help consumers take control of their data. Earlier this year we launched the second phase of our digital safety campaign which focused on data. The campaign sought to highlight the importance of personal data, shining a light on how consumers may be unwittingly sharing more data than they think, and highlighting how they can take a level of control that is right for them.

Consumer understanding will be critical to harnessing both the benefits that open data will bring, while ensuring the associated risks remain suitably managed.

3. Artificial Intelligence

While huge volumes of data are being created in our increasingly digital economy, it can be difficult for business to properly understand the data their consumers are generating. However, technologies such as artificial intelligence are being developed to help firms process, analyse and leverage their data to create value. Indeed, the huge volume of data being created is enabling artificial intelligence to advance at incredible pace, as systems hone their decision making as they process more data. In contrast to automation, the simple replacement of repetitive tasks by pre-programmed machines, artificial intelligence uses data to ‘think’, learn, and take action autonomously. This ability to respond without human involvement has the potential to transform how businesses operate and provide significant economic value.

Artificial Intelligence in Financial Services

AI is already making a major impact in Financial Services with firms experimenting with AI solutions to drive efficiencies, reduce costs, and improve the experience for customers and clients. Industry is experimenting with certain use cases, which we explore below.

- **Robo-advice** – Artificial intelligence has the potential to revolutionize the asset management sector, by removing the need for a financial advisor. A move in this direction would dramatically change current business models and significantly lower the cost of investing. As a result, AI has the potential to open up asset management to new market segments and user groups, enabling greater access to financial markets. Using its power to rapidly mine big data, AI generated advice and recommendations are more likely to be tailored to individual customers than human advice. AI powered robo-advice also has the potential to reduce human error and conflicts of interest as well as regulatory issues. Of course, it will raise new challenges such as ensuring they are designed to provide appropriate advice, and liability considerations, but the potentially benefits on offer should outweigh such challenges.

- **Consumer Engagement –** Firms are increasingly introducing 'chat bots' utilizing conversational AI systems and voice enabled technology to engage with customers. Using the power of big data and machine learning, chat bots can help respond to customer's questions, from on-boarding concerns to transaction-specific questions. In more sophisticated models, customer service chat bots can manage customer requests and make product recommendations. Chat bots have the advantage of being always accessible online, without ever requiring human interaction. AI powered chat bots are also less expensive to maintain than customer service telephone services, though chat bots will always be offered as a complementary service rather than a replacement.

- **KYC, Fraud Detection and Risk Management –** Using the power of big data, artificial intelligence has the capability to assess huge volumes of account and transaction data to detect possible fraud and potentially even identify areas of fraud before it happens. AI can significant boost bank efforts to reduce and prevent fraud on customer accounts therefore reducing the amounts spent reimbursing customers who have been victims of fraud. Instead, these funds can be invested in improving products and services elsewhere.

Challenges for Artificial Intelligence

As AI develops and its use by business increases, issues will likely emerge requiring policymaker intervention. Some potential challenges are explored below:

i. The Ethics of Artificial Intelligence

Now that the technology underpinning AI is sufficiently developed, public debate is shifting to the ethical considerations underpinning AI. Instead of considering whether outcomes can be feasibly achieved using AI and data technologies, increasing consideration is being given as to how those technologies may achieve an outcome, or indeed whether they should even be used for that purpose at all.

To ensure ethical development and use of AI systems, Government should develop a framework of guidelines for industry to abide by. In developing such a framework, it is important government engages all aspects of society to ensure it receives a diverse range of perspectives. For example, as well as academia and industry, it should engage civil society groups and consumer groups like Which? to ensure consumer attitudes to data and AI are understood.

Ethical concerns also cover the safety and security of AI. When AI systems are being designed it is crucial developers consider various ethical questions as well as their usual commercial concerns. For example, as well as considering what outcomes they want their AI system to achieve, and how it should achieve those outcomes, they should also consider potential societal impacts, and what would happen if the AI were to generate unexpected outcomes. Key concerns for government to consider regarding AI are:

- the societal impact of AI systems becoming better than humans at cognitive tasks, not just repetitive actions;
- the issue of AI programmed to undertake destructive actions;
- the impacts of AI programmed to achieve beneficial outcomes, but it develops its own destructive methods to achieve those outcomes.

It is critical that we develop the right ethical frameworks to assess how data is used as part of the AI systems, and to ensure there is fairness, accountability and reliability in the design process. Industry and government need to have clear visibility of the AI use cases being pursued and the rigour with which they are governed to minimise bias and undesired outcomes.

ii. Risk of Bias Within Artificial Intelligence

One of the most cited challenges regarding AI and data is the potential for bias in the system. While recognizing that no system will ever have access to perfect information, there is an inherent risk that AI frameworks, if fed by biased datasets, could lead to biased outcomes and potentially unfair or discriminatory 'decision making'. This is particularly significant for financial institutions with obligations to treat customers fairly. It is essential that firms looking to develop AI systems ensure to the maximum extent possible that any datasets they use are free of bias. Ultimately, any algorithm or AI system is only as valuable as the data being used to fuel it.

iii. GDPR and Artificial Intelligence

For all firms, the use of personal data in AI systems must be GDPR compliant. While protection of personal data is incredibly important, the restrictions on processing of personal data in GDPR may limit the potential benefit AI can offer and therefore the value it could create. For example, automated decision making restrictions (Article 22, GDPR) could prevent firms embracing AI to the maximum extent as significant manual (non-AI based) processes may still be necessary. It is important any decision making or processing based on AI is subject to strict human oversight and control, but potential efficiencies and benefits may not be realised if significant human intervention is required in each individual case. Government should therefore consider how automated decision making provisions under GDPR could be approached to enable AI and other technologies to deliver the most benefit.

iv. Liability

A key concern that remains to be dealt with is the issue of legal liability in the event that something goes wrong. While firms may develop their own AI systems, they also may acquire licenses for external systems, or simply outsource processing to third party firms. Currently, there is no clear framework setting out where liability lies. Government should therefore consider developing guidance or a liability framework setting out where liability would sit in the event that something goes wrong. As opposed to the unregulated sectors, financial services entities do still remain responsible for ensuring that they take reasonable steps to avoid undue, additional operational risk in connection with such outsourcing. However, there is currently no market standard or developed regulatory guidance in the area of testing AI.

v. Transparency, Explanation and Education of Artificial Intelligence

Public acceptance of AI technology is at an inflexion point. We continue to see a divergence in views and attitudes to AI between those who are advocates and keen to progress at pace, and those who fear the impact on jobs and are suspicious of the uses and applications of the technology. An adverse reaction to AI could limit the potential economic value the technology could provide. The pace at which technology is evolving and being integrated into day to day lives makes it imperative for us to focus on education and awareness of what the technology can do, what it cannot do and how to approach technology design and implementation in a responsible manner.

Education requires collaboration across industries and sectors. We welcome the creation of the AI Council with its remit to promoting adoption of AI in other sectors of the economy and have engaged them to support with our AI Frenzy events activity and emerging AI engagement and education initiatives we are developing. The investment in improving digital education at primary and secondary levels is key, and requires constant refreshing, given the pace at which technology innovation happens. It is also worth noting that the skill sets to understand and implement AI are not just limited to digital and computer science. The implication of using AI requires a multidisciplinary approach including humanities and creative skills to ensure that we are always aware of how the technology will interact with individuals and society. Government should consider how best to invest in AI education at schools and universities to ensure the UK has the right skills to lead going forward.

If AI is to deliver the value it has the potential to deliver, it is important consumers develop trust in the technology and its use. Transparency around the use of AI, and consumer understanding of its potential benefits are key to developing public acceptance, confidence and ultimately, trust. It is important consumers understand when they are engaging with AI, and when decisions are being taken on the basis of AI. One of Barclays AI Principles, that govern use and development of AI systems, stipulate that we will always be clear to consumers where they are engaging with AI and not a human.

There is a desire for transparency with regards to the AI design process. Under Article 22 of GDPR, financial institutions are required to communicate clearly with customers and regulators regarding AI / big data, including appropriate explanation of algorithms and how outcomes have been reached. For example, a firm may be required to explain how conclusions were reached in the context of a consumer credit assessment. However, this may be difficult to achieve in practice. Financial institutions are actively considering how, where, when, by whom and in what form, an explanation of AI's functionality should be documented, in the absence of guidance from regulators and any market standard.

4. Enabling Safe Data Sharing to Create Economic Value

The digitisation of markets has enabled the creation and storage of large amounts of consumer data with the potential to generate significant economic value for consumers and the wider economy.

Simultaneously, developments in technology and regulation are increasingly allowing consumers to control their data in ways never previously possible.

In financial services, the Open Banking framework provides a specific example of how, with the right Government, regulatory and industry collaboration, mechanisms can be put in place that enable consumers to share their data with competing third party providers.

Similarly, the new General Data Protection Regulation (GDPR) has enhanced consumers' control over their data, and introduced new data portability capabilities enabling consumers to transfer their data to competing providers.

Initiatives such as these create the foundations on which the UK can develop into a customer-centric, 'open data' economy, with greater competition as consumers leverage their data between providers for their own benefit.

Open Banking

The Open Banking framework, introduced following a Retail Banking Market Investigation by the Competition and Markets Authority, introduces 'Open Data' principles into financial services, providing consumers with the ability to securely share their financial data with third party firms, whilst continuing to retain their underlying relationship with their bank.

How Open Banking Creates Economic Value

The new framework provides opportunity for consumers to receive meaningful economic value by leveraging their personal financial data for their own benefit. Initial use cases have focused on account 'aggregation', whereby consumers will be able to view and manage their current accounts from different providers, all in one place. In the near future, consumers will be able to initiate payments from their accounts via the third party provider. Looking further into the future, consumers can expect to receive detailed analyses of their financial situation, along with personalised services and rewards. Indeed, in time, there is exciting to potential to further extend the framework to include other financial data to truly provide consumers with a comprehensive overview of their finances.

Lessons from Open Banking

The development of Open Banking has inspired a number of lessons which should be considered when developing similar data sharing frameworks or extending open data principles into other sectors.

- Critical to data sharing frameworks is how the data is transferred between entities, i.e., the mechanisms used to share the data. Open banking was designed to have customer security at its heart, and uses industry approved Application Programming Interface (API) technology to share customer data safely and securely with third parties. Importantly, this negates the need for consumers to provide their login credentials to third parties (known as screen scraping). With API technology underpinning the framework consumers can share their data with confidence, knowing they can stop sharing their data whenever they wish, by turning off the flow directly at their bank. Barclays strongly believes that API-based solutions provide the safest and most secure way of allowing consumers to share their data, and any future data sharing initiatives should be designed on this basis. The FCA is also supportive of this view as set out in its September consultation paper CP18/25 on forthcoming Regulatory Technical Standards for PSD2[1]

- It is also vital to ensure a common standard is accepted and adopted by all participants. Such a standard ensures that providers of new services have reasonable and consistent expectations over the data they will receive and the mechanisms by which this will be translated, preventing the need to build individual and bespoke interfaces to each data provider (for example, avoiding the iOS vs. Android dual app creation issue).

Open Banking represents the most significant change in retail banking in a generation, and has the potential to revolutionise how consumers manage their personal finances over the long-term. While still in its infancy, it is already showing signs of providing tangible benefits to consumers in the banking sector, and is proof that open data principles can be leveraged within the private sector to improve consumer markets.

Extension of Open Banking

There is potential to provide further economic value for consumers by extending the Open Banking framework beyond the nine largest banks, to include all banks. There will be consumers using challenger banks who would also like to benefit from all Open Banking has to offer, but currently their bank is not in scope.

Indeed, policymakers and regulators should consider how further economic value could be created through the introduction of similar data sharing frameworks in other data-rich sectors, for example the technology sector, using the Open Banking framework as a model.

Data Portability

The General Data Protection Regulation (GDPR) has enhanced the data protection framework in the UK and aligned regimes across the EU, strengthening consumers' rights over their data. One area strengthened is consumers' right to data portability, which has the potential to provide significant economic value to consumers and society.

The Economic Value of Data Portability

Under the new rules, consumers can request that firms provide back to them all data they have provided to the firm in return for a service, for the purpose of 'porting' it to a competing provider. This allows a consumer to switch service providers without losing their data profile developed with their existing provider and the associated benefits that brings. A consumer may be discouraged from

[1] https://www.fca.org.uk/publication/consultation/cp18-25.pdf

switching to a new service provider if, in so doing, they are unable to take their data history with them, and therefore have to begin creating a new data profile from scratch, which may disadvantage them – either in terms of product/service received or customer experience. Data portability has the potential to remove this barrier to changing service provider, therefore encouraging greater competition and enhancing economic outcomes for consumers. Alternatively, data portability could allow consumers to port their data profile to an intermediary to help them identify better services available at competing providers.

Where can Data Portability have the Most Impact?

Data portability is best placed to provide consumer benefit and economic value in sectors where consumers provide data over time, whereby they develop an extensive data profile that other providers can use to anticipate future behaviour, and tailor their service offerings. The insurance sector could provide a good example. Consumers provide a significant amount of data at the outset to receive a bespoke price quote. The need to 'recreate' their data profile with different providers could act as a disincentive to switch rather than renewing with their existing provider. Data portability in the insurance market could potentially act to help remove this barrier, potentially making it easier and simpler for consumers to switch providers to achieve the best cover at the best price.

More generally, we believe there are criteria that can be used to identify sectors that may be well positioned to benefit from data portability:

- markets rich in personal data, either through initial on-boarding, or through consumer activity;
- markets where data can be used to provide a tailored, personalised or cheaper service;
- markets in which there are multiple service providers.

Common Standards for Meaningful Data Portability

For data portability to fulfil its potential and provide maximum value to consumers there needs to be meaningful interoperability and agreement on common standards between market participants. The extent to which data is actually 'portable' to other providers is key. I.e. the data provided back to consumers should be properly readable, understandable and useable by different providers. Any requirement for the new recipient to prepare or process the data in anyway upon receipt will create extra friction and will naturally limit the potential of data portability. While GDPR dictates that data has to be shared in a commonly used format, if there are significant differences in what is provided by different service providers, the benefits available will be limited. Ensuring data is shared in as uniform a way as possible would contribute to the benefits of data portability being fully realised across the digital economy. It is therefore important that appropriate common standards are created, and adhered to by market participants. As the relevant useful data may differ between sectors, standardised data "templates" should be developed and agreed within sectors to ensure 'ported' data can be used without hesitation by different providers.

Consumer Awareness

For consumers and businesses to fully realise the benefits of data portability and other data sharing frameworks, the concepts need to become well established, be fully understood by consumers, and enjoy high levels of public awareness and trust. Consumer benefit will be limited if few consumers are aware of their right to data portability and the benefits that this can bring.

The government should therefore seek to maximise consumers' awareness of their data portability rights. Service providers should also be required to ensure consumers are aware of their rights and fully understand that they can request their personal data to share with other firms if they choose to.

Data Sharing Risks

While data sharing frameworks have the potential to create significant economic value, there may greater risks of fraud if frameworks are not secure. It is imperative that all data sharing is undertaken within a controlled, secure and transparent manner, as without such an approach, there is risk that data is shared in an uncontrolled way, leading to a markedly increased risk of customers being victim of fraud, scams and other negative impacts, as criminals seek to take advantage of a proliferation of available personal information.

In considering the issues and implications of greater data sharing, we have identified a number of questions (focused on retail financial services) that policymakers should consider going forward:

- In situations where the use of centrally held/coordinated data are necessary in order to access certain products or service (for example, credit scoring), what are policy makers' views on the possible scenario where a small number of private sector organisations hold the majority of such data?
- What are the minimum standards for data maintenance? What are the expectations on both consumers and the organisations that hold (and utilise) their data? Who has the right to update such data?
    - For example, if a 'data holding company' becomes aware that the data it holds on a customer is out of date (e.g. that they have moved address), but are not notified of this by the customer, is the organisation able (or, indeed, expected) to update the data without the customer's consent?)
- What if data on consumers is incorrect (either deliberately or accidentally) and becomes shared widely? Where does the responsibility sit for ensuring that these data are updated in a timely manner? What are the standards available to hold such organisations to account in situations where they do not meet these requirements, potentially resulting in customer detriment?
- If data shared is wrong and results in poor outcomes for a customer, who is liable – the sharer / or the company?
- If a fraudster assembles data from numerous sources and is able to de-fraud a customer who is responsible?
- Do consumers need a global 'do not share' instruction option for all companies they engage with?

5. Data Privacy and Protection

As the volume of consumer data, and its role in society increases, the importance of data privacy increases in parallel. Ensuring a strong data protection framework in the UK is critical to underpinning the move towards an open data economy.

Interoperability of Frameworks

While the UK currently has a world leading data protection framework in GDPR and the UK Data Protection Act, jurisdictions across the world are also updating and implementing their own frameworks of rules in parallel. As industry often operates across jurisdictions, and as it increasingly moves to using cloud storage and processing services based in jurisdictions across the world, there is a need to ensure data protection regimes are aligned, based on global standards, and where possible, allow for interoperability between jurisdictions. Government should therefore seek to lead development of global standards and push for interoperability between jurisdictions.

Innovation

As the digital revolution continues, it is important that innovation in the data landscape is balanced with and incorporates strong data protection provisions. Strong data protection will generate greater trust and willingness of consumers to provide their data to firms, or share data between firms, which will ultimately create even greater volumes of data in the system which can be leveraged for innovation. Greater volumes of data are beneficial to innovation, so ensuring strong data protection is ultimately in the interest of innovators.

Ensuring Privacy in Data Sharing

As discussed previously, greater volumes of data and data sharing frameworks have the potential to provide significant economic value to consumers. But as consumer data sharing increases, the risks to data privacy increase too, if that data sharing is not undertaken safely and securely.

Ensuring appropriate infrastructure and mechanisms are in place to share data is the best solution to facilitating data sharing, while limiting any risks to data privacy. Indeed, the API technology framework in place for data sharing within Open Banking is an appropriate model and a good example of how to share consumer data safely and securely. If data is not shared or ported securely, there is significant risk both to consumers in terms of data security, but also to the open data concept more broadly, as a major data breach may risk undermining data sharing initiatives before they have demonstrated their potential.

For Open Banking to have maximum impact and benefit to consumers, a cultural shift towards data sharing is required. For this to take place, consumer trust is key, and a strong data protection framework is crucial to underpinning that trust.

Distributed Ledger Technology and GDPR

As firms increasingly experiment with blockchain and distributed ledger technologies (DLT), Government should review how the technologies interact with GDPR and what they mean for ownership and storage of data, given in certain circumstances their decentralised model and lack of permission when data is shared. GDPR will likely raise significant challenges for DLT services. For example, 'the right of erasure' (Article 17) appears to conflict with the immutable nature of the blockchain, subject to further clarification on the term erasure. Further the legal concepts of "Data Controller", "Data Processor" and "Data Subject Access Request" will be become much more challenging to handle as copies of data are shared with all participants.

Data Adequacy

It is important to ensure the UK continues to be at the forefront of personal data protection going forward, as we leave the EU and beyond. As part of any Brexit deal, agreement will be needed on the treatment of data to maintain the current free flow of data that exists, or risk creating new barriers to the free flow of data across the new UK-EU border. The simplest solution would be a data adequacy decision under the GDPR framework. The Government should look to achieve such a decision from the EU as a priority matter.

Merchant Data Breaches

Naturally, as firms collect more and more data on consumers, and the value of data increases further, there will likely be an increase in the number of cyber-attacks intended to steal consumer data. Such data breaches in merchants of all sizes and across sectors will leave consumers exposed and vulnerable to fraud.

While the data breach may be the result of poor cyber security and data protection procedures of the merchant, it is banks that often have to incur costs to reimburse consumers of any fraudulent activity on their accounts, or incur costs of pre-emptive action like re-issuing compromised cards.

The Government should review the liability framework for merchant data breaches to ensure that those who allow data losses bear the full costs of those data losses, including any costs of third parties that can be accurately associated to their data loss. Otherwise, those who incur the losses will never have a full incentive to prevent them in the first place.

6. Data and Digital Trade

As international trade becomes increasingly digital in the 21st century, it is also important to consider the implications for data and cross border data flows in a digital economy.

The direction of travel in some jurisdictions is towards data localisation, i.e. the introduction of rules that effectively require data to be stored within national borders. For example, the Russian Data Protection Authority blocked access to LinkedIn to comply with a Moscow City Court ruling that LinkedIn had violated Russia's data localisation laws. There is a risk this becomes a growing trend, reflecting the increasing balkanisation of global markets as a result of national/jurisdictional regulatory action.

To halt this growing trend for data localisation, it is important to consider why jurisdictions are taking this approach. Some may have genuine concerns about privacy and security, a lack of trust in other jurisdictions, or perhaps a desire to create jobs and business in their jurisdictions. However, data localisation is a form of protectionism, and any small local benefit generated will be outweighed by raised costs and reduced access to global services for the economy as a whole. To help facilitate digital trade, it is important to address these concerns underlying data localization.

In this modern age with data becoming ever more important, it is vital that new borders are not created around our data, but that mechanisms and frameworks are in place to allow it to flow freely, and safely between jurisdictions. As any solution to this emerging problem needs to be global in nature, the Government should look to push back against any move towards data localisation on the international stage, and ensure an appropriate international framework exists in this space.