Australian Banking Association

# Treasury Laws Amendment (Consumer Data Right) Bill 2018

## ABA Response to the Exposure Draft

**07 September 2018**

**Pip Freebairn**

**Policy Director, Future Banking and Economics**

Australian Banking Association

# Executive Summary

ABA members support the introduction of a consumer data right that will encourage innovation and enable customers to benefit from data sharing while ensuring their privacy is safeguarded.

ABA members have been actively participating in the policy debate on data sharing and will be the first industry to be designated under the CDR. The ABA, on behalf of members, has participated in the Productivity Commission's *Data Availability and Use* report (**PC Report**) and Treasury's 2018 *Review into Open Banking* report (**the Farrell Report**).

The banking industry is now implementing open banking, with major banks required to share data from July 2019. The ABA is committed to working with the four agencies — the Australian Treasury, the Australian Competition and Consumer Commission, the Office of the Australian Information Commissioner, and Data61 — to design an appropriate system of economy-wide legislation as well as industry-based data sharing rules and technical standards. It is in this context that we have responded to the Treasury's exposure draft on the Treasury Laws Amendment (Consumer Data Right) Bill 2018. We have not commented on issues that will be covered in the rules and technical standards and are not intended to be covered in the legislation.

It is vital that the CDR system is designed to protect customers' privacy and that there is an avenue for redress if something goes wrong. This is to ensure that customers have full faith in the system and continue to use it as it is expanded across the economy. It is also important that businesses' incentives to innovate and invest remain, and that data sharing fosters competition rather than creating an uneven playing field.

This submission focuses on the key issues with the exposure draft that ABA members feel should be amended to ensure the CDR framework is successful. They are:

- Aligning the dataset definitions with the PC Report and Farrell Report and placing value-added data out of scope. The case for including value-added data in scope and the full implications of doing so, especially for customers, have not been fully explored.
- Designing a strong system of economy-wide reciprocity to ensure that the CDR system fosters competition and an even playing field, as well as to enable customers to access the full benefits of their data from across industries.
- Designing a system of privacy that protects both customers and businesses. Business and customers' rights and obligations under Australia's privacy laws, both inside and outside the CDR, must be easily understood for the CDR to be successful.

We thank Treasury for the opportunity to comment on this exposure draft and to participate in the consultation roundtables. We look forward to further engagement with Treasury and relevant regulators as the CDR system is designed.

Australian Banking Association

# Table of Contents


Executive Summary ..... i

1. The CDR framework and rule-making powers ..... 1

1.1 Value-added data ..... 1

1.2 Fee setting for data ..... 2

1.3 Emergency rules ..... 2

1.4 Transfer to non-accredited parties ..... 2

2. Reciprocity ..... 2

3. Privacy and rule-making powers ..... 3

3.1 The definition of CDR data ..... 4

3.1.1 Direct Marketing ..... 4

3.1.2 Voluntary data sharing arrangements ..... 4

3.1.3 Data holders' disclosures under the APPs ..... 4

3.2 The definition of CDR Consumer ..... 5

3.3 The role of the Office of Australian Information Commissioner ..... 5

3.4 Credit information ..... 5

3.5 Notification of CDR data security breaches ..... 5

3.6 Protection from liability ..... 5

3.7 Disclosure of government related identifiers ..... 6

3.8 Notification where data is found to be inaccurate ..... 6

4. Foreign entities ..... 6

5. Regulatory impact statements ..... 7

About the ABA ..... 9

Australian Banking Association

# 1. The CDR framework and rule-making powers

ABA members understand that the CDR must balance both flexibility and certainty to ensure that it is an appropriate framework across industries and into the future. But ABA members believe that the Consumer Data Right (**CDR**) exposure draft confers the rules making function with significant power that is largely not constrained and is only limited by the Australia Consumer and Competition Commission's duty to consult.

## 1.1 Value-added data

ABA members hold significant concerns that value-added and derived data have been included in scope for customer-directed data sharing. Neither the Productivity Commission's *Data Availability and Use* report (**PC Report**) or Treasury's 2018 *Review into Open Banking* report (**the Farrell Report**) recommended that value data be in scope. Both reports concluded that for the system of data exchange to be successful, it must encourage innovation and protect the intellectual property of data holders.

For this reason, ABA members seek clarification the specific datasets the legislation is seeking to include and the reasons behind doing so. ABA members also seek further clarity on the definitions of both value-added and derived data in the legislation and EM.

ABA members believe that data in scope should be limited to raw directly-captured basic data only. Data that draws on the proprietary insights of the institution holding the data — that is data that has been enriched or derived by the institution such as credit scoring models or other forms of intellectual property — should remain out of scope.

By including value-added data, the CDR is wider in scope than foreign regimes. For example, the European Union's General Data Protection Regulation (**GDPR**) only applies to the data that has been "provided by" the individual to the controller and was provided on the basis of consent.[1]

Guidance on the term "provided by" states that it will include personal data that relate to the data subject *activity or result from the observation* of an individual's behaviour, but does not include data *resulting from subsequent analysis of that behaviour*. This is relevant to considerations as to what *derived* or *associated data* is to cover and poses questions as to how these various (potentially confusing and therefore contradictory) distinctions will be made.

ABA members do not support the ACCC being given economy-wide powers to designate value-added data as part of a designated dataset. This imposes a significant degree of uncertainty for participants in the CDR regime that could be subject to providing data analytics they had developed through investments in their businesses. Rather than encourage innovation, as the CDR regime is intended to do, this could stifle innovation by discouraging business to develop analytics.

The practicalities of introducing value-added data also need to be considered. The ABA believes further analysis of the benefits to customers of including these datasets, as well as the full implications to customers of releasing specific value-added datasets. The ABA would like to be given the opportunity to consult with consumer groups on such situations.

The costs should also be considered. In banking, introducing value-added data significantly complicates the technical build required to deliver open banking, as value-added data sits on different systems to raw data.

In summary, the ABA believes that where a specific case can be made for value-added data to be shared, the specific named dataset should be included in the CDR dataset in legislative instrument when the industry is designated. There should be a clear and transparent process for making the assessment to include the value-added dataset, such as conducting a market study with industry consultation to assess the likely costs and benefits of including such data.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

## 1.2 Fee setting for data

The ability for the ACCC to set fees for data is an unusual power for the agency to hold and is largely without precedent. ABA members view that any fees charged to data recipients by data providers should be determined by market participants and not administered by the ACCC. Participants would have the usual avenues to appeal to the ACCC if they considered prices to be unfair.

The explanatory memorandum also leaves unclear the circumstances where fees could be charged for raw data, and we seek further clarity on these circumstances. We would support fees being charged, for instances, when data is being called by the data recipient at high frequency.

## 1.3 Emergency rules

Section 56BQ(1)(c) allows the Commission to make emergency rules without the consent of the Minister "if the Commission is of the opinion that it is necessary, or in the public interest to do so, in order to protect the efficiency, integrity and stability of any aspect of the Australian economy."

This is a broad power. Arguably, almost any issue could fall under the emergency rule and avoid consultation, as there is no materiality test or requirement for there to be an imminent risk of serious harm like sub(d).

The ABA recommends that the emergency power be limited to true emergencies by the following drafting change: "to protect *to avoid imminent risk of serious harm to* the efficiency, integrity and stability of any aspect of the Australian economy".

## 1.4 Transfer to non-accredited parties

The exposure draft and explanatory memorandum (section 1.47) enable CDR consumers to direct their CDR data to be provided in certain circumstances to a non-accredited entity. The ABA believes that CDR data should only be shared with accredited entities. Currently, banks have several bilateral data-sharing arrangements in place, such as sharing banking information relating to small business customers via accounting software providers.

Outside of these relationships, banks also have existing process for customers to ask for their financial data to be shared with third parties such as accountants. Given these arrangements, there seems no need to allow non-accredited parties to receive CDR data. Allowing CDR data to be transferred to non-accredited entities, however rarely, also risks undermining the customer protection which the accreditation process is designed to provide.

# 2. Reciprocity

The Government has indicated that the CDR has been developed to promote competition in industries like banking, telecommunications and energy by reducing barriers to entry to new entrants, thereby empowering consumers through greater choice of products and providers. However, in doing so, it is important that the framework does not distort competitive landscape and create new asymmetries between different types of market participants.

The Institute of International Finance's report Reciprocity in Customer Data Sharing Frameworks outlines the reasons for need for reciprocity to ensure fair competition fuelled by data (also attached in Appendix A).

The ABA is concerned that the principle of reciprocity has been watered down in the CDR Exposure draft to only apply to designated datasets.

ABA members strongly supported the comprehensive concept of reciprocity laid out in the Farrell Report. This would have required businesses from non-designated industries entering the CDR as data recipients to be required to share data that was deemed to be equivalent to the data they were wishing to receive.

This would ensure a degree of competitive neutrality for those participating within the regime, and importantly, would encourage a functioning economy of data exchange. It ensures that customers are able to fully utilise their data from across industries.

It is clear that designing a system of economy-wide reciprocity would require significant resources from ACCC and Data61. That is, necessary rules and technical framework would need to be established for any business that was seeking to self-designate by joining the CDR. While the ABA appreciates the resourcing pressure, we believe that reciprocity is vital for consumers to fully benefit from the CDR and to ensure fair competition between designated and non-designated industries.

Further work is required to scope how reciprocity extends into other industries, and a workable framework needs to be designed to designate datasets at the point of accreditation for non-designated entities wishing to join the regime. The ABA has commissioned legal advice on a workable solution that could be provided under existing law. We will pass this on to Treasury once available.

Finally, we make one observation on whether liability extends to data voluntarily provided under a CDR regime. The exposure draft creates uncertainty around if there is privacy protection for voluntarily provided data.

## 3. Privacy and rule-making powers

ABA members are supportive of a well-designed privacy system that protects customers' data by ensuring the proper use, access, disclosure or transfer, storage and deletion of CDR data.

The current drafting in the draft legislation provides that data recipients are generally subject to the Privacy Safeguards, which provide a more prescriptive approach compared to the Australian Privacy Principles (**APPs**). Under this model, data holders are subject to the APPs, except where specific Privacy Safeguards apply.

ABA members support the intended outcomes of the CDR's Privacy Safeguards, but at this stage, we believe the dual privacy system is too complex to work in practice, both for a consumer to understand their rights and for a business to understand its obligations.

Strong privacy protections are key to ensuring that customers can be confident to use the system. Both data holders and recipients face heavy penalties for breaches of the Privacy Safeguards so it is important that the rules be readily understood and able to be complied with.

Potential alternative models to that proposed in the draft legislation include drafting the Privacy Safeguards to build upon the APPs or turning off the APPs and replacing with the Privacy Safeguards. We believe further work needs to be undertaken to work through potential solutions and their full implications. We appreciate Treasury's acknowledgement of this issue and willingness to consult further to ensure that the Privacy Safeguards are appropriate and workable.

Care should be taken to ensure that the CDR's privacy obligations reflect the fact that they will operate in conjunction with existing legal obligations, such as confidentiality and privacy. This is pertinent given that:

- the banking sector is already regulated as to what information they collect for what purpose and the controls required to support the safe handling of that information in the course of the banking relationship; and
- the definition of CDR data under the current version of Section 56AF is very broad and forms the cornerstone of what datasets are in scope of regulation and therefore protections afforded under the Privacy Safeguards.

ABA members have identified several practical issues around the CDR and its Privacy Safeguards, and how they work in relation to the Privacy Act and Australian Privacy Principles (**APPs**). This list is not exhaustive.

## 3.1 The definition of CDR data

We note that in its summary of the issues arising from the stakeholder roundtables Treasury has stated that it is their intent "that the Privacy Safeguards should only apply in respect of the disclosure of CDR data in response to a CDR access request, and to the necessary steps to prepare CDR data for such disclosure."

ABA members believe that on the current drafting, a number of the Safeguards might also apply to CDR Data "at rest" with a data holder, that is CDR data that is collected and held in the ordinary course of business, and that has not been disclosed to an accredited data recipient at the request of a CDR consumer. Given the breadth of the definition of CDR data, this could apply to a very broad range of data "at rest".

Privacy Safeguards 5, 6, 7, 10 and 11 apply to the accredited data recipient and impose stricter requirements on the use of the data. However, given the data holder will continue to hold a copy of the CDR data (collected in accordance with the Privacy Act where it applies), it is unclear where the application of the APPs and the Privacy Safeguards will begin and end.

This poses several practical issues that ABA members have so far identified.

### 3.1.1 Direct Marketing

For instance, it is unclear if a data holder can continue to rely on APP 7 for **direct marketing** using personal information.

On the data recipient side, detail regarding direct marketing requirements for data recipients has been left to the consumer data rules. However, a data recipient may use or disclose CDR data for direct marketing where required or authorised by law. The corresponding APP 7 (which will continue to apply to data holders) does not include a general exception for direct marketing required or authorised by law.

This exception arguably gives scope for data recipients to rely on the lower consent standards under the Spam Act and the Do Not Call Register Act. It is not clear if this is intended.

### 3.1.2 Voluntary data sharing arrangements

In response to Treasury's request for suggestions on wording to narrow the Safeguards to achieve Treasury's intent and in order to ensure that the Safeguards do not restrict the ability of a data holder to enter into voluntarily data sharing arrangements outside of the CDR, we set out the following suggestion to *Section 56EF Privacy Safeguard 3 - collecting solicited CDR data.*

We are concerned that the current wording would restrict the collection of CDR data by ADIs who will be "persons who hold an accreditation under subsection 56CE(1)" from their clients as part of the products and services provided, and from third parties under voluntary data sharing arrangements outside of the consumer data rules.

We recommend that this is reworded to read as follows (amendment underlined):

*A person who holds an accreditation under subsection 56CE(1) must not collect CDR data <u>from a data holder</u> under the consumer data rules unless:*

*a) the collection occurs in response to a valid request from a CDR consumer for that CDR data to be so collected; or*

*b) the person's collection of the CDR data is required or authorised by or under:*

*i) an Australian law, other than the Australian Privacy Principles; or*

*ii) a court/tribunal order.*

### 3.1.3 Data holders' disclosures under the APPs

PS 6(1) limits the disclosure of CDR data by data holders unless required or authorised by the consumer data rules, a court/tribunal order or an Australian law other than the APPs.

The exclusion of the APPs seems impracticable here and may be a drafting error, as the EM says "it is not the intention that the CDR Privacy Safeguards restrict the ability of data holders to disclose CDR data outside of the CDR system where the disclosure is required or authorised under law, including under the Privacy Act."

Even if this is changed and data holders can disclose personal information as permitted by the APPs, this will still only provide an exception for personal information. Disclosure of CDR data about customers that are not individuals will be subject the stricter CDR regime.

One other possibility is that the government only intends PS 6(1) to apply to the disclosure to the accredited data recipient in response to the request, however this is not specified.

## 3.2 The definition of CDR Consumer

The definition of CDR consumer in section 56EI(1) as currently stated is broad and poses what appear to be unintended consequences that require drafting changes.

Data holders (and data recipients) must keep a note when relying on a basis other than the consumer data rules to disclose CDR data which has been requested by a CDR consumer (or associated CDR data). This may be difficult to comply with in practice as banks would make many disclosures of such data in the normal course of the banks' business.

In section 56H, it would require data holders to notify a significant number of individuals and companies identified in that dataset, which would make the CDR unworkable.

## 3.3 The role of the Office of Australian Information Commissioner

Given that the CDR data may relate to companies and individuals, the role of the Office of Australian Information Commissioner will be limited to matters that involve individuals and fit the legal definition of personal information as that term is defined under the Privacy Act 1988 (section 6) and interpreted by the Courts.[2]

## 3.4 Credit information

Further clarity is required to address how the CRD will operate with personal information that is also credit reporting information and is covered under Part IIIA of the Privacy Act.

## 3.5 Notification of CDR data security breaches

It appears section 56ER is intended to introduce changes to the Privacy Act to apply the mandatory data breach provisions to CDR data. Assuming that's the case and the changes are to be read into the Privacy Act, the new CDR definitions should also be specified as being read into the Act so the changes are properly interpreted.

## 3.6 Protection from liability

Section 56GC(1) provides protection from liability for the CDR participant where CDR data is provided in compliance with the *Competition and Consumer Act* Part IVD, regulations and the consumer data rules. The ABA believes that the data-sharing technical standards should also be expressly called out.

If a data holder or accredited data recipient fails to provide/collect data in accordance with the data standards, this could significantly increase risk of data breach. In such a case, there should be no protection from liability.

[2] Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017

## 3.7 Disclosure of government related identifiers

Disclosures of CDR data must not include government related identifiers (for example, driver's licence and passport numbers) unless required by a court or tribunal order or an Australian law other than the APPs or consumer data rules.

This provision potentially raises similar concerns to PS 6 in that banks may have other reasons to disclose CDR data independently of the CDR regime, and would now be subject to overly onerous and impractical disclosure restrictions. If the disclosure limitation here is confined to the disclosure to the accredited data recipient under the data request, that should be acceptable.

For clarity, it would help if the Bill specified that it only relates to government related identifiers of individuals. This is the better interpretation reading the Bill and the Privacy Act together, but there is still a degree of ambiguity.

## 3.8 Notification where data is found to be inaccurate

PS 10(2) imposes an obligation not found in APP 10. CDR participants that disclose CDR data under PS 6 must notify CDR consumers where the data is later found to have been inaccurate, incomplete, out-of-date or irrelevant.

The CDR participant is required to advise a CDR consumer in writing where it is "reasonably expected to be aware" that all or some of the CDR data was incorrect. The EM suggests this is only intended to apply where the initial disclosure is of inaccurate information, but this is not clear in drafting. The drafting could be improved to unequivocally connect the obligation to update back to the point in time of the disclosure. Take a routine example of a customer calling a bank to update their address or mobile number, section 56EM(2)(b) could be read to trigger a peculiar obligation for the bank to then advise the customer in writing of this same fact where it had previously disclosed this information under the CDR data request.

In relation to the obligation to advise the CDR consumer "in writing", this assumes the CDR participant continues to have a valid email or postal address. If, for example, the CDR consumer has since moved all bank products to a competitor, the data holder may not have current address information and could only use whatever was the last known. There is then no guarantee the CDR consumer will receive the advice.

Given the steep penalty, we suggest the section should be clearer and tighter to reflect known practice, perhaps by clarifying in this section that the CDR participant will be deemed to have advised the CDR consumer where it writes to the CDR consumer in accordance with this section using the CDR consumer's last known address/email address.

# 4. Foreign entities

The CDR draft legislation has been designed to enable data sharing to occur internationally. ABA members support customers being able to share data with foreign entities subject to there being redress for Australian customers if they face data breaches from foreign entities breaching their data.

Section 56AH aims to deal with the extra-territorial application of Part IVD of the Competition and Consumer Act 2010. We note that the use of the term "collected" is broad in scope. This section could be further defined to reflect that CDR designated data should specifically relate to data captured in systems owned by companies in Australian, for the purpose of the relationship held in Australia.

Some scenarios include:

- A foreign bank in Australia outsources its credit card operations to a contact centre offshore. Customer information is updated in to the banking system of the foreign bank in Australia by the offshore team. ABA members believe this data should be in scope.
- A foreign bank in Australia and its foreign parent share a mutual customer. The foreign parent has potential CDR designated information in their banking system that is not present in the

systems of the foreign bank in Australia. ABA members believe this data should not be in scope.

- A customer in Australia has an account with bank in Australia and also holds an account with that bank's affiliate in New Zealand. The data from the New Zealand account sits in the bank's Australian systems, as there is a servicing agreement on behalf of the affiliate in New Zealand. ABA members believe this data should not be in scope.
- A foreign bank in Australia has a customer who also has an account with an affiliate in the UK. The foreign bank in Australia's staff can see the UK account balances. ABA members believe this data should not be in scope.

## 5. Regulatory impact statements

The Regulatory impact statement and review of the CDR should take place more frequently than once every three years. The regime should be reviewed by Treasury each year for the first three years, and necessary refinements be made where appropriate.

Australian Banking Association

# Appendix

See attached - Institute of International Finance's report Reciprocity in Customer Data Sharing Frameworks

Australian Banking Association

## About the ABA

With the active participation of 24 member banks in Australia, the Australian Bankers' Association provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services.

The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

INSTITUTE of INTERNATIONAL FINANCE

JULY 2018

# RECIPROCITY IN CUSTOMER DATA SHARING FRAMEWORKS

## 1. INTRODUCTION

In the new digital economy, products and services are based on data like never before. New technologies have exponentially increased the capabilities to store, process and transfer data, and a large amount relates to the behavior and characteristics of consumers. The utilization of this data has led to greater personalization of products, services, marketing and advertising; indeed, the fact that many digital services are offered at a 'zero-price' to the consumer — in exchange for the information generated while using them — demonstrates the value of data in the digital economy.

The massive increase of data processing in the digital economy involves risks for privacy and security, among others, and has driven policy and regulatory initiatives around the rights of the data subjects and the obligations for the firms that control and/or process data. Some of these regulations are introducing 'mandatory customer data sharing frameworks' that allow clients to transfer their raw data[1] from one firm to another, thus requiring companies to put in place the appropriate mechanisms to make this right effective. Cross-sectoral examples of this include the new right to portability of personal data found in the General Data Protection Regulation (GDPR) in Europe, while financial sector-specific examples include 'Open Banking' regimes, which includes developments such as the new Payment Services Directive (PSD2) in Europe, the Open Banking standard in the UK, the new FinTech law in Mexico. Although some jurisdictions are clearly following this trend, as shown in the Annex, there are some others where data sharing frameworks remain a voluntary business decision within each firm's strategy.

This paper outlines the rationale and main features of mandatory data sharing frameworks — as required by regulations — and draws special attention to some of the unintended consequences if they create asymmetries between different types of participants that may distort fair competition in digital markets.

## 2. DATA SHARING FRAMEWORKS

Mandatory data sharing frameworks are generally driven by one or more of the following objectives:

- promoting overall competition by reducing the barriers to entry to some markets and facilitating switching between providers. For instance, historical consumption data can be used to make a more personalized offer to a potential customer; or, when data is part of the service itself, such as in social networks, users can reduce the lock-in effect by transferring their images, posts or messages to a new provider;
- empowering consumers with greater control over their data, in line with the spirit of data protection and privacy rules, bringing them greater value from their own data;

[1] Raw data includes data provided by the customers as well as data generated from their use or consumption of products and services. In contrast, non-raw or elaborated data (which is produced by firms taking raw data as an input) should not be included under mandatory data sharing frameworks to preserve the firms' incentives to invest in data quality and analytics.

- facilitating innovation in data-based services, which underpins competition and choice, by allowing firms to gain access to new sources of data (i.e. information generated in the context of the customers' relationship with other parties) to which they can apply Big Data analytical techniques.

The effective contribution of mandatory data sharing frameworks to these objectives critically depends on the specific features and implementation of each framework, as well as on the extent to which customers exercise their new rights. Mandatory data sharing frameworks require firms to make data portable, but the customers are the ones that determine the extent to which they share their data across firms.

As shown in the Annex, data sharing frameworks can vary significantly depending on the entities obliged to make data shareable; the type of customers entitled to share data; how data is shared between the parties; and the entities with which data can be shared. For instance, whereas the right to personal data portability under GDPR has a cross-sectoral scope, data sharing under PSD2 is limited to payment account data (but also affects business customers, not only individuals). In addition, the timing of the data sharing (real time vs. deferred) and the standardization of transmission mechanisms (e.g. APIs) make a huge difference between both frameworks in terms of the usability of data and, therefore, the potential contribution to the previously described objectives.

## 3. POSSIBLE COMPETITION IMPLICATIONS

When the entities obliged to make their customers' data shareable and those with whom data can be shared differ, data sharing frameworks may create unfair asymmetries between players. This is the case in the emerging open banking frameworks, such as the UK Open Banking Standard or the EU PSD2, which make payments information (part of the banks' core customer data) accessible to non-bank players.[2] Those non-bank players, on the contrary, do not have similar requirements to make their own core customer data (which typically differs from payments) shareable with third parties, including banks.

The asymmetry or lack of reciprocity means that a regulation intended to facilitate the entrance of new players and promote competition and end-user choice in the payments market has created a competitive disadvantage for banks and other financial services firms vis-à-vis players from other industries. This risk contributing to the existing trend in digital markets towards the concentration of power in the hands of a few big technological players.[3]

In this regard, it is important to note that digital markets are blurring the traditional boundaries between industry sectors, including financial services. There are predominately two reasons for this. First, the nature of some digital products grants them control over services in other markets (e.g. mobile operating systems and application marketplaces over mobile payment services such as digital wallets). Second, the accumulation of customer data not only provides firms with a competitive advantage in the markets where they operate (e.g. by allowing them to improve the quality over time), but also allows them to develop and/or distribute other products and services. Data gathered from the provision of one service has value in other markets, and increasingly so with more advanced data analytics based on artificial intelligence.

In this context, it has been argued that making customers' data portable (i.e. through introducing mandatory data sharing frameworks) can help to preserve and promote competition in the digital economy and empower consumers to access new and more personalized products and services across multiple industries, including

[2] To access payments data under PSD2, non-bank players shall be registered as "account information service providers" and comply with some basic governance, internal control, financial and security requirements, as well as having professional indemnity insurance or a comparable guarantee.

[3] Some digital markets tend towards high levels of market concentration due to the presence of strong direct and indirect network effects as well as data-related economies of scale.

financial services.[4] However, this needs to occur equally across sectors so as to not accidentally distort competition further.

## 4. ALTERNATE MODELS TO ACHIEVE DATA RECIPROCITY

Where data sharing asymmetries across different types of market participants exist under some open banking regimes, there are some alternate models for how this might be addressed.

One scenario would be restricting data sharing requirements to intra-industry participants, so that only the firms making their core data shareable (e.g. banks, in the case of PSD2) are those able to get access. While conceptually this is a reciprocal scenario by definition, one downside is that it would create a sort of 'data closed loop' among certain industry players, as opposed to having broader approach to ensure that the full potential of data can be taken by all market participants.

In a more open approach, the raw data held by companies in all industries would be accessible by any firm on similar terms (i.e. in real time), when requested by the customer. Banks would have to make accessible transactional data from credit, savings or investment products, while other companies would have to do so with their respective raw data (mobile phone records, online search queries, social media content, etc.). This would enable all the entities nominated by the client to have access to the same amalgamated data pool, from which they could each run their own analytics and compile their own respective offerings to the customer. To avoid introducing an additional compliance burden for smaller firms, these could be exempted from the legal obligation to have data sharing mechanisms (e.g. when they have a database below a certain level, such as 50,000 customers).[5]

While it is speculative as to whether customers would choose to exercise the option to share other data items, such as their internet searches or social media interactions, this could serve as a catalyst for customers to better understand and interrogate the data that the big digital players currently hold on them. This could also help to drive better data literacy, and importantly to empower consumers via a far greater understanding of the value of their personal data to companies. They will in the end be able to provide authorization to access specific data based on the value-added proposals from market participants.

Amongst firms, this approach would also incentivize (and reward) those that make investments in greater data analytical capabilities, both removing barriers and allowing firms to compete openly without any differentiation by their respective entity-type. It is acknowledged that this may have different impacts over large and small players: while it can be argued on one hand that smaller firms may be challenged to keep up with the investments in analytical capabilities to extract value from data, it is also true that the 'net potential gain of data' (information provided vs. received) is much larger for smaller players.

From a regulatory perspective, this open scenario could be implemented in different ways. On the one hand, sector-specific regulations (such as the EU's PSD2 or the Mexican FinTech law) could be developed in parallel across industries, making data from different sectors mutually accessible. On the other hand, a single cross-sector regulation could be introduced, such as the EU's GDPR with its data portability right.

---

[4] As highlighted in the study from the Association of Information Services (AIS) together with the University of Passau (Germany) entitled "Data Portability on the Internet: An Economic Analysis", data portability (as an overall impact) will foster market entry, improve innovation and service variety

[5] The California Consumer Privacy Act of 2018, for example, states that any business should share the data they held if one out of three different requisites applies. One of those is that "Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"

In any case, the challenge is how to develop standardized communication mechanisms and data taxonomies, along with robust authentication mechanisms, that make these frameworks effective and usable in practice. The issue of data taxonomies is particularly challenging given the great variety and dynamism of products and services in the digital economy and the types of data involved.

In this regard, Application Programming Interfaces (APIs), are methods of standardizing data exchange that are already widely used both within and between firms.[6] 'Open APIs' are therefore increasingly seen as one of the best-practice ways of implementing mandatory data sharing frameworks, indeed they form the base of all the Open Banking frameworks proposed to date.

The different alternate models for achieving reciprocity have a mix of pros and cons, and neither is necessarily the perfect model. Each would enable a form of more balanced competition, and they would remove the anomaly that currently exists under some open banking initiatives that create unfair asymmetries between players, even though they are increasingly competing for the same customers in the digital economy.

## 5. CONCLUSIONS

The central role data plays in the digital economy has driven regulatory and policy interventions around the world regarding the access to and the use of customer data. In this regard, a number of jurisdictions are introducing mandatory data sharing frameworks that allow customers to transfer their data from one firm to another, with the aim of promoting greater competition, facilitating innovation in data-based solutions and empowering customers with more control over their data.

As the so-called "new oil" of the digital economy, data has value across industries, and indeed is contributing to blurring up the boundaries between traditional sectors. Precisely because of this, perhaps the most relevant characteristic of any data sharing framework should be the symmetry and reciprocity in the access to data (i.e. that the entities obliged to make their customer's data shareable and those with which data can be shared are effectively the same). This can be reached either through sector-specific closed data sharing frameworks or more open data sharing frameworks across sectors.

Reciprocal data access is particularly important due to the potential for concentration in digital markets, where a few big players are accumulating huge datasets, and whose business model is mainly powered by their capacity to extract the highest value from data. Asymmetric data sharing frameworks, such as the EU's PSD2, provide them with access to more data, while maintaining exclusivity over their own datasets. This may further increase concentration in digital markets and ultimately harm consumers if it reduces competition and, therefore, the incentives to innovate, improve quality and keep prices low.

Ultimately, any data sharing framework should satisfy a number of minimum requirements to become a reality:

- Customer data control: customers have control over their raw data, and decide what they will share, with whom and for what purpose.
- Transparency: clarity on who controls and processes the data in question and the reasons for doing so, providing the customer with the tools to authorize and manage access accordingly.[7]

[6] APIs are generally defined as a set of procedures that allow one software application or service to access the features or data of another application or service.

[7] As BaFin states in its recent study on 'Big Data meets artificial intelligence', "consumers can only make a sovereign decision if they are adequately informed about the potential reach and consequences of the use of their data, if they are given reliable options for controlling how their data is used, and if they have actual freedom of choice".

- Security: customers must have absolute confidence about the security of their data, both in terms of sharing it with third parties and the manner in which it is stored.[8] Their focus should be understanding the value of their data and the benefits of sharing them.

- Incentives: the different stakeholders of the data sharing ecosystem need to have the right incentives to actually share their data (in the case of customers) and to build value added proposals for customers based on those shared data (in the case of service providers).

Reciprocal data sharing frameworks that follow these principles will ensure fair and dynamic competitive landscapes, and in the end, they will benefit the customer through better, more personalized and price efficient proposals from a broader range of providers. This is key for developing and unleashing the full potential of the digital economy.

[8] For a detailed explanation of the importance of security in data sharing frameworks, see the recent IIF paper 'Safeguarding Customer Data in the Financial Sector'.

ANNEX: Key features of mandatory data sharing frameworks

| | Open Banking (UK) | PSD2 (EU) | GDPR (EU) | Open Banking (Australia) | Open API Framework (HK) | FinTech law (Mexico) |
|---|---|---|---|---|---|---|
| Entities obliged to make data shareable | Nine largest retail banks. Others can also choose to participate | Account servicing payment service providers (including banks) | Any firm controlling personal data | Banks[9] | Banks | Banks, money transmitters, credit bureaus, crowdfunding and e-payments institutions |
| Customers entitled to share data | Individual and business customers | Individual and business customers | Natural persons | Individual and business customers | Retail customers | Individual and business customers |
| Data that can be shared[10] | Transactional data from current accounts; to be extended to all payment accounts | Transactional data held in payment accounts | Personal data observed by the firm or directly provided by the individual | Customer provided data and transactional data | Account information and transactions across core banking | Transactional data |
| When data is shared | Real time | Real time | Within 30 days | Real time | Real time | Real time |
| Standardization of the transmission | Using mandatory standardized APIs | Only basic standardization is mandatory[11] | No standardization is mandatory | APIs will be developed, but screen scraping will not be forbidden | Various internationally recognized standards | Standardized APIs (pending definition) |
| Entities with whom data can be shared | Authorized payment service providers, including banks and service-specific entities | Authorized payment service providers, including banks and service-specific entities | Any other firm | Banks[9] and third parties (based on a graduated, risk-based accreditation standard) | 3rd party service providers that enter into bilateral contractual relationships | Entities obliged to make data shareable and authorized IT specialized third-parties |

[9] Authorized Deposit-taking Institutions (ADIs), which includes banks (other than foreign bank branches), building societies and credit unions. Obligations will be phased in, beginning with the largest ADIs.

[10] Some of these regulations or frameworks include other open banking functionalities such as making product or reference data publicly accessible or allowing third-parties to initiate payments on behalf of customers. However, information on the table is limited to the sharing of customers' data.

[11] According to the European Commission (EC) FinTech Action Plan, it will help to develop more coordinated approaches on standards for FinTech by Q4 2018 and will support joint efforts by market players to develop, by mid-2019, standardized application programming interfaces that are compliant with the PSD2 and GDPR.

**Brad Carr**
Senior Director, Digital Finance Regulation and Policy
bcarr@iif.com

**Daniel Pujazon**
Policy Advisor
dpujazon@iif.com

**Pablo Urbiola**
Policy Advisor
purbiola@iif.com