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