Organisation for Economic Co-operation and Development

DSTI/CDEP/DGP(2021)1/FINAL

Unclassified English - Or. English

10 January 2022

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Data Governance and Privacy in the Digital Economy

Mapping data portability initiatives, opportunities and challenges

JT03488022

Foreword

Data portability has become an essential tool for enhancing access to and sharing of data across digital services and platforms. This report explores to what extent data portability can empower users (natural and legal persons) to play a more active role in the re-use of their data across digital services and platforms. It also examines how data portability can help increase interoperability and data flows and thus enhance competition and innovation by reducing switching costs and lock-in effects.

The report was drafted by Christian Reimsbach-Kounatze, Andras Molnar, Suguru Iwaya, and Elettra Ronchi (all from the OECD Secretariat). Lauren Bourke and Holly Ritson contributed to earlier drafts of this report. The report was prepared under the aegis of the OECD Committee for Digital Economy Policy (CDEP), with input from delegates of the Working Party on Data Governance and Privacy in the Digital Economy. Delegates to the DGP and CDEP provided valuable feedback. The report builds upon three expert workshops and a survey of business practices. The support of the Danish Business Authority is gratefully acknowledged.

This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy (CDEP) on 1 October 2021 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on ilibrary as:

OECD (2021), "Mapping data portability initiatives, opportunities and challenges", *OECD Digital Economy Papers,* No. 321, OECD Publishing, Paris, https://doi.org/10.1787/a6edfab2-en.

Table of contents

Tables

Figures

Boxes

Executive Summary

Overview

This report explores to what extent data portability can empower users (natural and legal persons) to play a more active role in the re-use of their data across digital services and platforms. It also examines how data portability can help increase interoperability and data flows and thus enhance competition and innovation by reducing switching costs and lock-in effects.

Findings

Data portability has become an essential tool for enhancing access to and sharing of data across digital services and platforms. This report shows that current data portability arrangements by government and private sector differ significantly along five key dimensions:

- *Sectoral scope,* including whether they are sector-specific or horizontal and thus directed potentially at all data holders regardless of the sector.
- *Beneficiaries,* including whether only natural persons (individuals) or also legal persons (i.e. businesses) have a right to data portability.
- *Type of data that is subject to data portability arrangements,* including whether data portability is limited to personal data and whether it includes volunteered, observed or derived data.
- *Legal obligations,* especially the extent to which data portability is voluntary or mandatory and if the latter, how it is enforced.
- *Modus operandi,* or modalities of data transfer, meaning the extent to which data transfers are limited to or include ad hoc (one-time) downloads of data in machine-readable formats (regarded as “data portability 1.0”), ad hoc direct transfers of data to another data holder (“data portability 2.0”), or real-time (continuous) data transfers between data holders that enables interoperability between their digital services (“data portability 3.0”). Another important modality is whether third-party data recipients need to be accredited to participate in data portability arrangements.

Whilst data portability may bring about considerable benefits, it also may carry risks. For instance, while data portability can increase competition, consumer choice and data-driven innovation, it may also generate unintended adverse effects on market structures and dis-incentives to invest. Data portability can facilitate data flows and data sharing, but transferring data to destinations not controlled by the original data holder can increase digital security and privacy risks.

There are also a number of implementation challenges for individuals, businesses and regulators:

- *Uncertainties regarding the scope of data portability initiatives*. The significant differences across data portability initiatives, including in terms of their purpose, scope (who has the right to have data ported; what data can be ported, including in cases where data refer to third parties; whose data should be portable) have introduced significant uncertainties for market participants and users.

- *Digital security and privacy risks and liabilities*: Freeing up the transfer of personal data may increase personal data flows, but also increases digital security and privacy concerns. There should be clarity on the circumstances under which the data holder or the data recipient may be held liable for incidents.
- *Lack of interoperable specifications including standards and application programming interfaces (APIs)*: Even when commonly used machine-readable formats are used, in the absence of common standards, interoperability may not be guaranteed. APIs – the software specifications used to facilitate communication and data sharing between information systems – can help implement the necessary safeguards, including for identity management, and reduce the necessity of "data scraping".
- *Costs of compliance:* Most compliance costs are generally one-off expenses for implementing data portability rather than for ongoing operations. They may include technical costs for developing or accessing a secure API; transactions costs associated with getting consents from other data subjects when data are related to multiple parties; and legal costs such as compliance audits and regulatory fines.
- *The need for cross-agency regulatory and enforcement co-operation*: Data portability initiatives address issues at the intersection of competition, privacy and consumer protection. Other regulatory domains may also be concerned where data portability is implemented at a sectoral level (e.g. open banking). As data portability initiatives may span multiple regulatory domains, governments need to plan which regulator will have primary oversight of the initiative to ensure efficiency, streamlined processes and beneficial outcomes. There is also an increasing need for co-operation across the various regulatory and policy areas.

Conclusions

- **More work is needed to develop common standards and interoperability:** Governments should promote standards for data portability and interoperability requirements. Trusted third parties can then help implement these standards.
- **More awareness about benefits can clarify issues of liability and obligations**: Governments should raise awareness among the public about the benefits of data portability. This should further clarify liabilities and obligations of the original data providers and recipients. It should also strengthen cross-agency regulatory enforcement co-operation and co-ordination.
- **Third parties can help develop new business models:** Trusted third-party intermediaries can stimulate the creation of new business models around data portability that reduce transaction and compliance costs. This could include helping to reduce costs for data holders and recipients to ensure compatibility with different technological specifications and costs to create numerous data links for portability, standards, interoperability and compatibility.
- **Increased centralisation of data transfer schemes needs risk analysis**: An expanding role for intermediaries will drive the centralisation of data transfer schemes, potentially creating risk related to competition, privacy and consumer protection. Analysis is needed to better understand the potential implications of such centralisation and if the criteria for "trusted" intermediary should be re-assessed.
- **Cross-agency co-operation is needed to regulate data portability**: There is increasing need for cross-agency regulatory co-operation and co-ordination, especially in areas where data portability is cross-sectoral. In most cases, data portability involves personal data and can be motivated by privacy, consumer and competition enforcement considerations. This requires multidisciplinary enforcement collaboration, particularly when other sector-specific regulators are concerned.

Mapping data portability initiatives and their opportunities and challenges

Introduction

OECD (2019[1]) highlights the importance of online platforms for daily social and economic activities and the increasing dependence of individuals, businesses and governments on them. The work also identifies the common economic characteristics of online platforms,[1] including the extent to which they rely on the collection, control and use of data (including, but not limited to, personal data). Online platforms take advantage of direct and indirect network effects, as well as increase returns to scale and scope enabled by the collection, control and use of data. These capacities have raised concerns about the switching costs and lock-in effects that online platforms (can) generate to the detriment of their users, including individuals and organisations.

Similar to *number portability* that enables telephone users to retain their telephone numbers when changing from one network carrier to another, data portability may foster interoperability of data-intensive products and reduce switching costs between platforms. Data portability could thus reduce market-leading firms' ability to exploit the "stickiness" of their products to reinforce their market positions ("lock-in effects"). While data portability is much more complex than number portability, it might enable data users (both consumers and businesses) to change more easily to new and potentially better data-intensive goods, services and platforms. This, in turn, might foster greater user choice, competition and innovation.

Data portability has thus been highlighted as an essential tool to promote the sharing and re-use of data across digital services. At the same time, it can strengthen control of individuals over their personal data and of businesses (especially small and medium-sized enterprises [SMEs]) over their business data. Prominent data portability initiatives include the "My Data" initiatives of the United States begun in 2010, the "midata" data portability initiative of the United Kingdom in 2011, and, more recently, the "Right to Data Portability" (Art. 20) of (European Union, 2016[2]) General Data Protection Regulation [GDPR], and Australia's Consumer Data Right [CDR]).

Data portability initiatives are in line with the 1980 OECD Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188] (hereafter, the "OECD Privacy Guidelines"), revised on 11 July 2013 [C(2013)79, C/M(2013)15/REV1]. The OECD Privacy Guidelines include a right to access (the individual participation principle) that provides that individuals "should have the right to obtain from a data controller, or otherwise, confirmation of whether the controller has data relating to them [and] to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them" (OECD, 2013[3]). The original Explanatory Memorandum explained that the

"right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard" (OECD, 2013, p. 58[4]). However, the individual participation principle does not require data controllers to share that data with other controllers. In other words, it does not encompass all of the elements commonly understood as data portability today.[2]

As highlighted in this report, data portability is user-centric: data portability puts the user, whose data are concerned (typically the data subject), in control of access and sharing. This characteristic has been critical in the midst of the COVID-19 pandemic, as it empowers users to share their sensitive personal data at their discretion. Some countries have therefore explored means to leverage data portability to enhance access to, and sharing of, data to combat the pandemic. Although elaborated prior to the COVID-19 pandemic, changes proposed to the Privacy Rule set out in the Health Insurance Portability and Accountability Act (HIPAA) of the United States would allow individuals to directly share their health care data between health care provider and health plans (HSS, 2020[5]; HSS, 2020[6]; Black, 2021[7]). This includes changes mandating the provision of electronic patient health information under specific circumstances to individuals at no charge (Black, 2021[7]).

Objective and structure

This report aims to develop a common understanding of data portability. It offers a working definition for data portability, and most importantly, a taxonomy through which data portability arrangements and initiatives can be further differentiated and categorised. This taxonomy is then used for mapping data portability initiatives in the private and public sector.

The report then discusses to what extent data portability can be a means for empowering users (natural and legal persons) to play a more active role in the re-use of their data across digital services and platforms. It also explores to what extent data portability can help increase interoperability and data flows and thus enhance competition and innovation by reducing switching costs and lock-in effects. Data portability, however, also raises a number of risks and challenges, which the report also analyses. These include digital security, liability and privacy risks; the costs of compliance; and possible unintended negative effects on innovation (by potentially lowering incentives to invest) and on competition (by potentially discouraging market entry). The report concludes with key policy challenges that require more attention and possible areas for further work.

Methodology

In addition to the desk research that helped inform this report (including in respect to data portability initiatives), this report draws on discussions and main points emerging from a series of expert consultations (hereafter "Online Expert Consultations"). The first consultation – the OECD Online Expert Discussion in Preparation for OECD Expert Workshop on Data Portability – was held on 17 April 2020. This event enabled experts to share their understanding of data portability, and to identify and further explore some key benefits, opportunities, risks and challenges concerning data portability. This event led to the OECD Online Expert Workshop on Data Portability on 6 November 2020. The Online Workshop focused on a potential typology of data portability initiatives and on the barriers to effective implementation.[3] These events were followed by a Hearing on "Data portability, Interoperability and Competition" (jointly organised with the Competition Committee) and the Webinar on Data Portability [DSTI/CDEP/DGP(2021)7], held on 9 and 10 June 2021, respectively.

The report also benefited from responses to an OECD survey in 2020 to gain a more thorough understanding about the data portability initiatives of online platforms[4] (hereafter "Online Platform Survey"). In particular, the questionnaire aimed to examine the data portability initiatives of 12 of the world's major online platforms.[5] Of these initiatives, five companies (Airbnb, Apple, Facebook, Google, and Rakuten)

responded. The analysis of these responses helped provide insights on the implementation challenges faced by these firms. The questionnaire is reproduced in Annex B.

Understanding data portability

Data portability is often regarded as a promising means for promoting data access and sharing, while strengthening control of individuals over their personal data and of businesses (in particular SMEs) over their business data (Productivity Commission, 2017[8]). It is therefore considered a useful approach for enhancing access to and sharing of data (EASD).

For this report, data portability is understood as the ability (sometimes described as a right) of a natural or legal person to request that a data holder[6] transfer to the person, or to a specific third party, data concerning that person in a structured, commonly used and machine-readable format on an ad hoc or continuous basis.

This section highlights how data portability relates to, but also significantly differs from, other types of EASD approaches and examines its unique characteristics. This includes why the term "data portability" should be reserved for EASD approaches with these unique characteristics. The section then offers a possible working definition for data portability and a taxonomy through which data portability arrangements and initiatives can be further differentiated, categorised and analysed. This taxonomy will be used in the next section for mapping data portability initiatives in the private and public sector.

Data portability as an approach for enhancing access to and sharing of data

Data portability is one of many approaches for EASD. As highlighted in OECD (2019[9]), these EASD approaches fall across a continuum of different degrees of data openness, covering various forms of conditioned access to data and open data arrangements (Figure 1). Data portability may be considered a specific form of conditioned data access and sharing arrangement, namely one through which a specific stakeholder accesses data (see Level 1 in Figure 1), typically the data subject (i.e. the individual that is identified or identifiable through personal data).

Figure 1. The degrees of data openness and access

Source: (OECD, 2019[9]).

In other words, under data portability, data holders are required to provide conditioned access to data, in a commonly used, machine-readable structured format, either to the user, whose data are concerned, or to a third party chosen by the user. The provision of data in this format is, however, not specific to data portability. This kind of format is a technical minimal requirement of all EASD approaches, including open data (OECD, 2018[10]; OECD, 2020[11]; OECD, 2019[9]; OECD, 2019[12]).

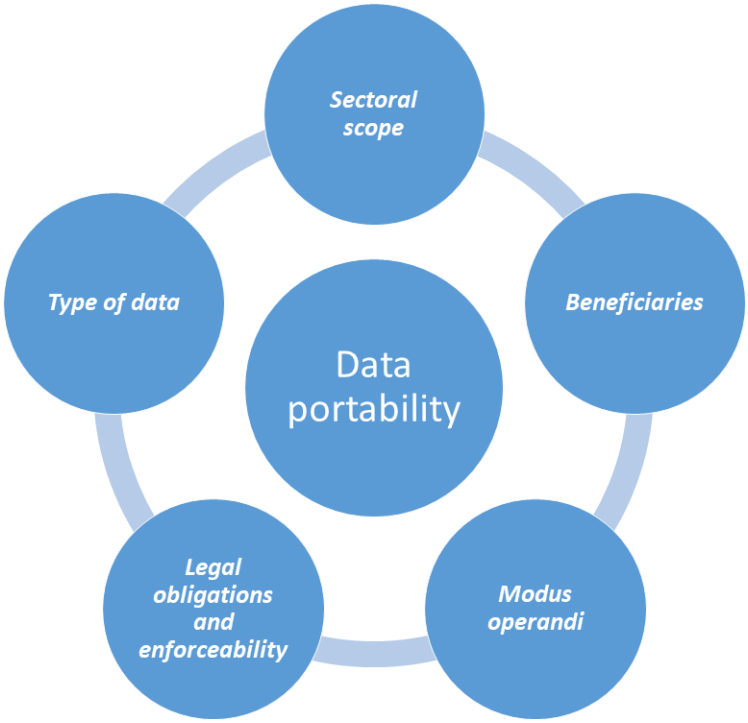
Data portability offers a user-centric approach by putting the user, whose data are concerned (typically the data subject), in control of its access and sharing (Lynskey, 2017[13]; Janal, 2017[14]; Graef, Husovec and Purtova, 2018[15]). The user typically initiates the transfer of data by the data holder, whether directly to the user or to another data holder. This contrasts with other EASD approaches, where data subjects do not initiate the data transfer but can only consent or not to such transfer (where the law requires consent).

The key dimensions of data portability: Towards a taxonomy of data portability arrangements

In the last decade, governments have adopted an increasing number of data portability initiatives. In addition, the private sector, including online platforms, has recognised that such initiatives respond to an increased desire from users to enhance control and, where requested, to share and re-use data about them across digital services. These data portability initiatives vary significantly across jurisdictions in terms of their nature, purpose, scope (who has the right to have data ported and what data can be ported), requirement and implementation.

While there are significant differences, some data portability arrangements and initiatives share some commonalities. The following five key dimensions can be used to categorise data portability arrangements and initiatives (Figure 2). Combined, they provide a taxonomy that will be used in the next sections for mapping and analysing data portability initiatives in the private and public sector.

Figure 2. Key dimensions of data portability initiatives



1. *Sectoral scope*: Whether data portability arrangements or initiatives are sector-specific and thus only directed to data holders in a specific sector or are horizontal and thus directed potentially at all data holders across sectors and domains.
2. *Beneficiaries*: Whether only natural persons have a right to data portability (excluding legal persons i.e. businesses) or whether also legal persons (i.e. businesses) have a right to data portability.

3. *Type of data subject to data portability arrangements*: whether data portability is limited to personal data and whether it includes or excludes volunteered, observed or derived data.
4. *Legal obligations*: The extent to which data portability is voluntary or mandatory, and if so, how it is enforced.
5. *Modus operandi*, especially in respect to the modalities of the data transfer, meaning the extent to which data transfers are limited to or include ad hoc (one-time) downloads of data in machine-readable formats (data portability 1.0), ad hoc direct transfers of data to another data holder (data portability 2.0), or real-time (continuous) data transfers between data holders that enable interoperability between their digital services (data portability 3.0).[7] This also includes the extent to which third parties receiving the data (third-party data recipients) need to be accredited or not.

Other dimensions could also be used to categorise data portability arrangements but are outside the scope of this report. For example, data portability regimes could also be classified based on whether data portability consists of an *ex ante* or an *ex post* regulatory measure. Data portability measures discussed in this report are primarily *ex ante* measures. In contrast, *ex post* measures are typically those specific to competition enforcement. These arise where data portability may be considered as a remedy after an antitrust violation is revealed. In this case, data portability would typically be mandated by a regulator or the relevant court (Box 1) [see also (OECD, 2021[16])].

Box 1. Data portability as (*ex post*) competition enforcement remedy

Data portability is often considered one of the *ex ante* regulatory measures that complement competition law remedies in policy discussions on competition issues. These include discussions on digital platforms in areas such as digital advertising, web search and social media (CMA, 2020[17]; ACCC, 2020[18]; HDMC, 2020[19]). Data portability can also be considered as an *ex ante* measure in merger reviews. However, the large majority of such cases tend to focus on requiring merging firms to license (bulk) data access instead of data portability as defined in this report (FTC, 2014[20]).

In general, *ex post* competition law remedies have a number of advantages over *ex ante* regulatory measures. These include minimal compliance costs due to targeted enforcement, greater flexibility and coverage over all types of data when used for facilitating data mobility (OECD, 2020[21])(para. 41). This is highlighted when considering the potential benefits brought about by digital innovations for not only innovators but also the economy and society more generally. For instance, platforms can help customers find better services and products, as well as help start-ups and SMEs overcome their relative disadvantages in capital investments and geography, and enable their market access. In addition, digital markets can develop in unpredictable ways. Consequently, blanket *ex ante* regulation that applies to all market participants can impose overbroad restrictions or costs on markets that ultimately do not exhibit competition concerns. This, in turn, can inhibit innovation unnecessarily (JFTC, METI, MIC, 2019[22]).

However, when faced with systemic competition issues common in the digital economy, such as those under review by a number of jurisdictions, governments have begun to consider complementary *ex ante* regulatory measures. Fast moving markets in the digital economy can generate adverse competition effects that may cause large-scale harms before competition law investigations and interventions are completed. In digital markets, network effects and high switching costs, for instance, may facilitate the exponential growth of a particular platform, thereby concentrating market share (and market power over its users) with that platform. In addition, efforts to investigate may be hampered if potential competitors also rely on services offered by the dominant platform and are reluctant to co-operate with investigators All these challenges are exacerbated by complex networks of value chains in the digital economy and algorithmic transactions embedded in software codes (e.g. real-time auctions for advertising slots on

search engines). Such networks may increase the difficulties for third parties and authorities to prove adverse effects on competition and consumer welfare (CMA, 2020[17]; HDMC, 2020[23]; HDMC, 2020[19]).

To tackle the competition issues that may be raised by the characteristics of digital platforms described above, governments are considering *ex ante* measures that address governance of platform operators, as well as data-related remedies such as data portability. Because the latter may have fundamental impacts on competition, careful consultation with stakeholders and long-term analysis and monitoring are needed (CMA, 2020, pp. 350-351[17]). Measures to increase data portability are also considered for increasing consumer control over data and reducing the barrier to entry and expansion.

Sector-specific vs. cross-sectoral approaches to data portability

A major distinction should be made between general cross-sectoral or horizontal data portability approaches, and sectoral approaches. General cross-sector or horizontal data portability approaches include EU GDPR, California Consumer Privacy Act (CCPA) of 2018 and the California Privacy Rights Act (CPRA) of 2020. Conversely, sectoral approaches include the United Kingdom's Open Banking Initiative and the Payment Service Directive for Payment Businesses in the European Union (PSD2). The latter are most frequently used in infrastructural sectors, including financial services (open banking and the EU Second Payment Service Directive of November 2015 [PSD2]), transportation and mobility (the EU Regulation on Motor Vehicles of May 2018), energy (e.g. EU Electricity Directive of 2019) and health care (e.g. HIPAA).

Australia's CDR is also used most frequently in infrastructural sectors, even though it is best classified as a hybrid approach in this respect. The CDR is implemented at a sectoral level based on requirements defined with market participants (primarily in infrastructural sectors such as banking, energy and telecommunications). However, it is a horizontal framework that ensures a common approach across sectors.

Horizontal data portability initiatives tend to focus on a specific type of data, most prominently personal data. In other words, "there are no data [portability] rights that are guaranteed across sectors for all data types" (Specht-Riemenschneider, 2021[24]). In a recent study of the EU legal framework on data portability, CERRE (2020[25]) made this same observation. The study shows that horizontal data portability initiatives focus either on personal data or non-personal data (see Table 1), with competition law being the exception in many respects (see Box 1). Sector-specific data portability initiatives, on the other hand, will tend to cover a range of data types.

Table 1. EU legal frameworks for data portability and sharing

	Personal data	Non-personal data
Horizontal	Art. 20 GDPR – Right to data portability	Art. 16 Digital Content Directive – Obligations of the trader in the event of termination
		Art. 6 Free Flow of Data Regulation – Porting of data
Sector-specific	Art. 66(4) and 67(3) – Second Payment Service Directive (PSD2)	
	Open Banking initiative in the United Kingdom	
	Art. 61 Regulation on Motor Vehicles (2018) – Access to vehicle diagnostic, repair and maintenance information	
	Art. 23(2) New Electricity Directive	

Source: (Krämer, Senellart and Streel, 2020[25]).

At both the OECD Expert Discussion on Data Portability and the OECD Workshop on Data Portability, experts underlined the reasons to consider sectoral approaches over horizontal approaches to data portability. They highlighted that sector-specific approaches could better address the specific legal, organisational and technical requirements of individual sectors, given that requirements for data transfers may vary by both data type and sector. Cross-sectoral data portability approaches might not foster competition and innovation effectively.

Cross-sectoral approaches may nonetheless facilitate data sharing both across sectors and within sectors more effectively. This becomes possible as certain industries may not have sufficient incentives to develop a user-driven, data-sharing framework on their own. Several experts also noted that sector-specific approaches may create asymmetries. In these cases, certain businesses may act as data "gatekeepers", while others are required to share their data. As an illustration, the revised PSD2 enables non-banks to access consenting clients' payments data when they are authorised as third-party providers. However, banks are not given similar access to the comparable data sets, which could lead to unfair competition. As Kerber (2021[26]) explains

> One of the important critical concerns is with the danger that large digital tech firms (e.g. Apple, Google) can use this data access for entering the market with potentially negative effects in the long term. Since these large platform firms do not have to open their data, demands for reciprocity of data access have emerged. *(de la Mano and Padilla, 2018[27]; Di Porto and Ghidini, 2020[28])*

The beneficiary

Most data portability initiatives focus on individuals as the only beneficiary of the right to data portability. This reflects the common rationale of most data portability initiatives, namely the desire to empower individuals, particularly consumers. It is especially the case with privacy and data protection frameworks that include a data portability right, such as the EU GDPR and the CCPA/CPRA.

However, more recent initiatives also allow consumers (including organisations) to request that a data controller transfer their data to the user or to a third party. Australia's CDR, for instance, extends the right to certain businesses (not just individual data subjects). More specifically, the legislation defines one of its three categories of actors as "CDR consumers", which can include either individuals or small businesses. CDR consumers can hold rights to access data held by data holders (the other category of actor) and direct that data be shared with accredited data recipients (the third category of actor).

Similarly, the EU Free Flow of Data Regulation (FFDR) (European Union, 2018[29]), promotes data portability of non-personal data in B2B relationships. "The Regulation instructs the Commission to contribute to the development of EU Codes of conduct to facilitate the porting of (non-personal) data in a structured, commonly used and machine-readable format including open standard formats" (Krämer, Senellart and Streel, 2020[25]). The EU FFDR aims, among other goals, to enable easier switching between cloud service providers for professional users. The European Commission has been working with stakeholders on "facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can move data between cloud service providers and back into their own IT environments" (European Commission, 2021[30]). One of these codes of conducts – on cloud switching and data portability – was developed by the working group on switching cloud providers and data porting (SWIPO). It was presented at the High-Level Conference on Data Economy in December 2019 during the Finnish EU Presidency (see Box 2).

Box 2. SWIPO's codes of conduct for data portability and cloud service switching

In 2019, the working group on switching cloud providers and data porting (SWIPO), which counts 26 members including EU and non-EU based cloud service providers, finalised the development of two codes of conducts (CoCs) on data portability and cloud switching. These relate to, respectively, Infrastructure as a Service (IaaS) cloud services (SWIPO, 2020[31]) and Software as a Service (SaaS) cloud services (SWIPO, 2020[32]).

In respect to data portability, the IaaS CoC states a number of requirements and recommendations to identify the technical measures that would support "the process of porting Infrastructure Artefacts". It recommends, for example, that "the cloud service shall be capable of importing and exporting CSC Infrastructure Artefacts, in an easy and secure way, (…) The Infrastructure Cloud Provider (Infra. CSP) shall provide the support to enable the transfer of Infrastructure Artefacts using structured, commonly used, machine-readable format" (SWIPO, 2020[31]).

The requirements and recommendations of the SaaS CoC are more specific to data portability. They aim "to support safe portability and/or migration of data in the effective switching between cloud services providers and between cloud service providers and cloud service customers' own IT services" (SWIPO, 2020[32]).

Apart from two dedicated CoCs, the SWIPO working group also delivered an extensive proposal for a governance structure. As foreseen by the Regulation on the free flow of non-personal data (FFD), the European Commission will evaluate the impact of those CoCs on the fluidity and competitiveness of the cloud market before November 2022.

Source: (European Commission, 2021[33]; SWIPO, 2020[31]; SWIPO, 2020[32]).

The type of data subject to data portability arrangements

Data portability initiatives vary significantly based on their scope, in particular in regard to which data should be made portable. Work on EASD and data governance to date has shown that policy makers should not treat data as a monolithic entity but differentiate between different types (OECD, 2015[34]; OECD, 2019[9]). Data portability initiatives will also have to, to the extent they do not already, distinguish between different types of data to address various stakeholder interests. What types of data should be made available through data portability initiatives? The answer must distinguish, for instance, between personal data, proprietary (private) data, and public (including public domain) data. These three categories can and do overlap, reflecting stakeholders' often conflicting interests when it comes to data portability (OECD, 2019[9]).

More importantly in the context of data portability, the OECD (2019[35]) distinguishes between:

- *Volunteered (or surrendered, contributed or provided) data* is data provided by individuals when they explicitly share information about themselves or others. Examples include creating a social network profile and entering credit card information for online purchases.
- *Observed data* are created where activities capture and record data. In contrast to volunteered data, where the data subject is actively and purposefully sharing its data, the role of the data subject in the case of observed data is passive; the data controller plays the active role. Examples of observed data include location data of cellular mobile phones and data on web usage behaviour.
- *Derived (or inferred or imputed) data* are created by data analytics processes, including data "created in a fairly 'mechanical' fashion using simple reasoning and basic mathematics to detect

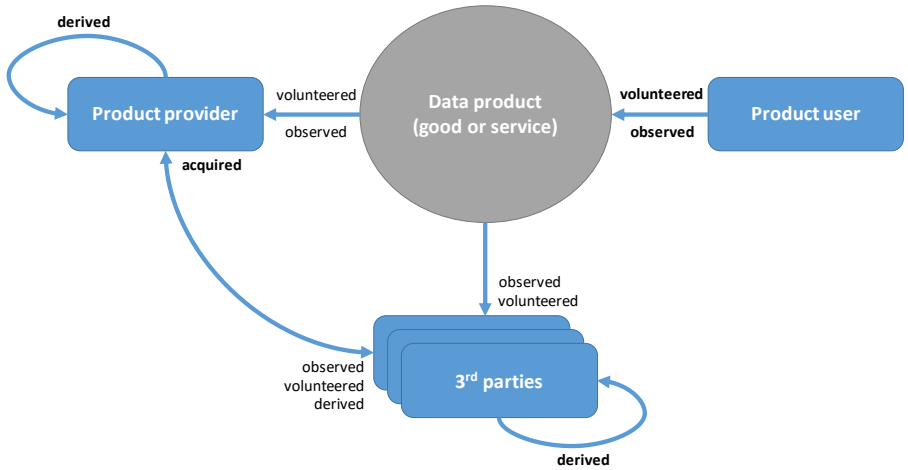
patterns" (OECD, 2014[36]). In this case, the data processor plays the active role. Data subjects typically have little awareness over what is inferred about them. Examples of derived data include credit scores calculated based on an individual's financial history.

- *Acquired (or purchased or licensed) data* are obtained from third parties based on commercial contracts or licences (e.g. when data are acquired from data brokers) or other non-commercial means (e.g. when data are acquired via open government initiatives). As a result, contractual and other legal obligations may affect the re-use and sharing of the data.

This categorisation reflects the extent to which different stakeholders are involved in the creation of data. This includes cases where users (consumers and businesses) interact with a data product (good or service) such as a social networking service or a portable smart health device (Figure 3). Data portability initiatives tend to focus primarily on volunteered data and to some extent on observed data. Some uncertainties remain on whether observed data should be subject to portability rights (see section below on "Implementation challenges").

The GDPR right to data portability, for instance, only applies to personal data "provided by" the data subject with consent or under contract that is electronically processed. The (former) Article 29 Working Party indicates in accompanying guidance that the definition of provided personal data should encapsulate data volunteered by the individual, as well as *observed* by virtue of their use of the service or device. However, it should not include personal data that is inferred or derived (OECD, 2015[34]). Australia's CDR more explicitly distinguishes between i) data posted on line by the consumer (including individuals as well as SMEs); ii) data created from online transactions; iii) purchased data; and iv) "other data associated with transactions or activity that is held in digital form" (Productivity Commission, 2017[8]). Depending on the industry, the type of data made available to consumers may vary significantly, reflecting sector-specific risks and needs. In the case of the banking sector, for instance, volunteered data will be made available, as well as data on financial products such as credit and debit cards, deposit and transaction accounts, and data on mortgages.

Figure 3. Data products and the different ways data originates



Note: Arrows represent potential data flows between the different actors and a data product (good or service). The type of data is highlighted in bold to indicate the moment at which the data are created.
Source: (OECD, 2019[9]).

Responses[8] to the Online Platform Questionnaire suggest that online platforms allow their users to download and port their data to other platforms. A respondent specified they allow users to port data that may include their profile information, pictures, videos, posts, comments and group memberships. Another

online platform created a portability product that provides a central site for users to export and download their data. The service facilitates the export of data for numerous products. Users can export their data in a variety of industry-standard formats they may select based on the product, service and intended use. This online platform highlighted that allowing users to download their data in multiple formats provides flexibility and creates many options for their use. Given the different data portability regulations across regions, an online retailing platform indicated each of its local services is responsible for fulfilling data portability requirements (depending on the jurisdiction where the data portability request was made). In those cases where the data may be linked, data portability is provided to the user for those services to which they are connected.

Modus operandi

Data portability is commonly characterised by the provision of data in a structured, commonly used and machine-readable format. However, the structured and machine-readable data can be provided to the user in many different ways. This can typically include the following two mechanisms:

- *(Ad hoc) downloads*, whereby the data are stored (in a commonly used machine-readable format) and made available on line (e.g. via a website). This mechanism raises a number of issues, especially data interoperability. Even when commonly used machine-readable formats are employed, data interoperability, and hence the re-use of the data, is not guaranteed (OECD, 2019[9]). These formats may enable *data syntactic portability*, i.e. the transfer of "data from a source system to a target system using data formats that can be decoded on the target system". However, they do not guarantee *data semantic interoperability*, defined as "transferring data to a target such that the meaning of the data model is understood within the context of a subject area by the target". In addition to common machine-readable data format, data semantic portability requires mutually understood ontologies and metadata to assure a common meaning of the data. Furthermore, data downloads are typically only suitable, for one-time access, but not for continuous real-time data portability.
- *Application programming interfaces (APIs):* As applications increasingly rely on data, accessing data without human intervention becomes essential. Application programming interfaces (APIs) enable service providers to make their digital resources (e.g. data and software) available over the Internet.[9] APIs thus enable the smooth interoperability of the different actors, their technologies and services, particularly through the use of cloud computing. APIs come with a number of advantages:
  - Compared to an ad hoc data download, an API enables a software application (or app) to directly use the data it needs. It is thus suited for continuous real-time data portability.
  - Data holders can implement several restrictions via APIs to better control the use of their data, including means to assure syntactic and synthetic portability.
  - Data holders control the identity of the API user, the scale and scope of the data used (including over time). They even control the extent to which the information derived from the data could reveal sensitive/personal information. APIs are therefore increasingly being used even for one-time data portability downloads and transfers between data holders.
  - A dedicated API or avenue through which to send and receive data may reduce the perceived necessity of "data scraping" (or "screen scraping"). This is a practice of giving a third party one's credentials to grant them access to an online account and "scrape" the data from the online interface and, in some cases, to execute transactions on the customer's behalf. In this way, data portability regimes that take advantage of APIs can increase the security of, and trust underpinning, data transfers.

By considering how data are provided, including mechanisms for these transactions, data portability initiatives can be categorised according to the extent to which they encourage or mandate the adoption of

the above mechanisms to enable data portability. This adoption can take place either through ad hoc downloads (data portability 1.0), ad hoc direct transfers of data to another data holder, typically via APIs (data portability 2.0), or real-time continuous data transfers that enable interoperability of digital services via APIs (data portability 3.0).

The delay between the user's request and the transfer of data is another consideration. For example, Article 12(3) of the GDPR requires that the original data holder provides the data subject with information on action taken in response to a request "without undue delay" and in any event within one month of receipt of the data subject's request. This one month period can be extended to a maximum of three months for complex cases where the data subject has been informed about the reasons for such delay within one month of the original request. In contrast, the CCPA requires that businesses that receive a verifiable request from a consumer must

> promptly take steps to disclose and deliver, free of charge to the consumer, the customer's personal information (…) by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. (California Civil Code Section 1798.100[d])

As another example, PSD2 provides that

> (t)he account servicing payment service provider shall: (…) (b) immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider.

Data portability arrangements may also distinguish the types of data recipients, in particular whether third-party data recipients need to be accredited to receive data. Australia's CDR, for instance, limits participation to third-party data controllers that have demonstrated particular security measures to ensure the security of any personal data they receive (OAIC, 2021[37]). To be able to receive consumer data, third-party data recipients must be accredited by the Australian Competition and Consumer Commission (ACCC). Once accredited, they are referred to as "accredited data recipients" (ADRs) or "accredited providers" and can "use a CDR brand mark to help consumers recognise that the business is able to receive their data securely and manage it in line with the rules and safeguards of the CDR system" (OAIC, n.d.[38]).

Responses[10] to the Online Platform Questionnaire show that respondents have implemented basic functionalities to enable data portability (1.0). This includes tools through which users may obtain a copy of their data in human-readable (HTML) and machine-readable (JSON) formats. Some online platforms centralised their data portability functions so that users can access in one place all the data provided across multiple online platform services.

One online platform indicated that the data are sometimes sent directly to certain competing services on the users' requests (data portability 2.0). Some survey respondents also participate in the Data Transfer Project (DTP). They noted this project aims to develop tools and interoperable models to enable users to request secure, privacy protective, direct data transfers between services without needing to download and re-upload data.

Data portability: An interim step toward interoperability?

EASD is sometimes motivated by interoperability considerations. There is almost always a need for better interoperability, where data are to be shared and re-used. This is particularly the case with data portability arrangements because they give users the right to receive the data provided in a structured, commonly

used and machine-readable format, and to transmit those data to another data holder. Interoperability is not a legal obligation under most data portability initiatives (with the exception of some data portability 3.0 initiatives). However, data portability may foster interoperability of data-intensive products. As a result, it could reduce switching costs to such an extent that businesses can no longer fully exploit the "stickiness" of their products to reinforce their market positions (lock-in effects) (see next section below).

Interoperability can have different meanings depending on the context. Generally, it is understood as compatibility, such that systems can work together or "interoperate" in a way that allows for seamless or real-time exchanges, updates or transfers of information or data. In relation to cloud computing, the International Standards Organization (ISO) defines "interoperability" as the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged (ISO, 2017[39]). In the context of policies promoting consumers to switch products, services and providers, interoperability includes organisational aspects. For example, the United Kingdom's gas and electricity regulator defines interoperability as the ability of diverse systems, devices or organisations to work together (interoperate) in the design of smart metering implementation. Then, interoperability is decomposed into functional, technical and commercial interoperability (Ofgem, 2010[40]). Furthermore, interoperability can apply also to consumers' technological choices, changes in component devices and changes in suppliers' value chain (Catapult Energy System, 2018[41]).

A recent EU report on "Competition in the Digital Age" defines two types of interoperability that are relevant to discussions about digital competition and data portability: (full) protocol interoperability and data interoperability (Eurostat, 2019[42]).

- *Protocol interoperability* is used similarly to the ISO definition. Examples of protocol interoperability include e-mail systems, by which users can send and receive e-mails to other users despite using different e-mail services, and computer or mobile operating systems. In competition contexts, protocol interoperability is often referred to as a means to address market power. Full protocol interoperability is described as a means by which "two or more substitute services interoperate" completely (European Commission, 2019).
- *Data interoperability* is defined as "roughly equivalent to data portability but with a continuous, potentially real-time, access to personal or machine user data". Generally, data interoperability is achieved via APIs as described above (Eurostat, 2019[42]).

Nicholas (2020[43]) refers to data interoperability as "API interoperability" and describes it as a form of data portability. This is contrasted with "one-off" data portability (1.0 and 2.0) as is contemplated by data portability rights such as that found in Article 20 of the GDPR and similar frameworks (Nicholas, 2020[43]). Data interoperability requires data controllers to maintain an ongoing relationship via the API. Nicholas (2020[43]) notes that APIs allow "the receiver [to] get data faster and more often [and] also lets the data sender observe and control what, when and how the receiver gets data". In this context, data either exist or are transferred or exchanged in a mutually understood format or are translated to a common format via the API. However, commonly used machine-readable format may guarantee only syntactic data interoperability but not semantic interoperability (OECD, 2019, p. 32[9]). Further, APIs may promote data flow and data standardisation, including of associated metadata. However, issues remain as to API standardisation and consensus among industry participants (Gal and Rubinfeld, 2019[44]) (see section below).

Data interoperability has been recognised as an enabling factor for competition between platforms. The European Commission, for instance, has focused on interoperability in the context of addressing competition in digital markets, "as we believe it to be one of the instruments that can keep markets open" but noting that "[t]he emergence of ecosystems and the complementarity of services with one another and with devices is an important, but not yet very well researched, element of competition" (Eurostat, 2019[42]). The Japan Fair Trade Commission has noted that "even if platforms enable data transfer or open access

to data, unless data interoperability is ensured, pro-competitive effect through data transfer would be reduced" (JFTC, METI, MIC, 2019[22]).

Data portability can help foster competition as discussed further below thanks to the benefits of interoperability. These benefits include: i) reducing barriers to entry, where market entry relies on access to competition-relevant data, enabling external firms to compete to provide (competing and over the top) services and products (Eurostat, 2019[42]); ii) reducing switching costs for users, in particular where significant network effects reduce incentives of users to switch providers (Gal and Rubinfeld, 2019[44]; Brown and Korff, 1 October 2020[45]); and (iii) enabling multi-homing, as, rather than simply switching to a new service following a porting event, users can continue to use both the original and new service as the same data are made available in both contexts (Nicholas, 2020[43]).

While interoperability has competitive advantages, fostering it through additional requirements to facilitate data portability can also have negative effects on competition. Protocol interoperability implemented within ecosystems, such as operating systems, without any requirement to allow interoperability with external actors can reduce competition as it increases switching costs. Data interoperability, to the extent that it requires adherence to specific IP protected standards or APIs, can introduce or raise barriers to entry. These barriers include increased costs of compliance with standards or API compatibility.[11] This is especially the case where foreign companies may be required to comply with national or regional standards to interoperate (Gal and Rubinfeld, 2019[44]). This, in turn, can have limiting effects on innovation. Nicholas (2020[43]), for instance, notes that "competitors may be hesitant to build a product that depends on incumbent APIs out of fear that the incumbent will change them or cut off access". This concern was noted around Facebook API functions such as "invite Friends" and "Publish actions", which allow users of third-party apps to invite users to Facebook and can automatically push posts to Facebook (CMA, 2020[46]). The concern was also noted in relation to the Google Maps API (US House Judiciary Committee, 2020[47]).

Interoperability achieved via APIs can often result in development of products similar to the originator data controller's product. This ultimately reduces the incentive for users to switch to competing offers from new entrants (Nicholas, 2020[43]). This is consistent with a phenomenon observed in Singapore. New digital banks can gain a small market share of 1-5% of the unsecured retail and SME loan market in Singapore. However, it is more natural for small banks to pursue a platform-based business model rather than compete with large banks by providing similar products (Choy, 2020[48]).

The opportunities of data portability and their associated risks

This section discusses in greater depth the various rationales for data portability. These include data portability as a means to i) increase competition and consumer choice; ii) stimulate data-driven innovation and markets for new data products and services, including new online platforms; iii) facilitate data flows and data sharing; and iv) achieve "informational self-determination" by strengthening individuals' control over their data.

The latter three and, in particular the ability of data portability to facilitate data flows and data sharing, underline that data portability is also a means for third parties to collect data. This implies that data portability also comes with a number of risks to privacy and personal data protection. It therefore needs to be implemented with appropriate safeguards and limits. These should be in line with the collection limitation principle and the purpose specification principles of the OECD Privacy Guidelines (OECD[49]).

The Online Expert Discussion, which was designed to draw out the above-mentioned opportunities, confirmed that many opportunities come with their respective risks. Increasing competition, consumer choice and data-driven innovation, for example, may come with the risk of possible unintended adverse effects on market structures and incentives to invest. Facilitating data flows and data sharing can give rise to attendant digital security risks, including the risk of data breaches. Finally, achieving informational self-

determination may give rise to privacy risks, including from over-collection of data. To this end, consumers could also be pressured to provide their data, which could be used against their interests.

As participants in the Online Expert Discussion stressed, policy makers need a clearly defined use case that will frame discussions about the development of standards for data portability initiatives. It also needs to incorporate clearly defined objectives. This will ensure a regime is easier to develop, more efficient and more effective in the medium and long term. Naturally, the nature of data portability initiatives vary (e.g. horizontal or sector-specific; applied to traditional sectors like energy and mining or digital online services), and different measures have distinct risks and opportunities. The following section highlights both the benefits and the possible risks and challenges generally associated with data portability.

Increasing competition and consumer choice, and unintended adverse effects on market structures

Opportunities: From reducing information asymmetries to reducing barriers to market entry

In the early 2000s, the concept of "mobile number portability" gained traction. Mobile number portability allows subscribers to keep their unique telephone number in one or more of three situations: when they move from one location to another ("location portability"), when they change telecommunications services (such as from fixed telephone services to mobile in some countries – "service portability") and when they change to a new telecommunications provider ("operator portability"). One rationale behind number portability was to remove the disincentive of losing one's phone number when switching providers. This aimed to increase competition among operators and enable the exercise of consumer choice.[12] A major difference with data portability, however, lies in the content of what is being ported. Whereas phone numbers are simple and easily controlled, data portability often relates to large quantities of data, indeterminable to an average consumer.

Data portability is widely regarded as a promising means for increasing competition between providers of digital goods and services, including platform providers. Initiatives such as Australia's CDR, and to some extent the EU's right to data portability in the GDPR, emphasise that data portability could increase competition between providers of goods and services. This potential has led to discussions about the extent to which businesses should be granted data portability rights in some OECD countries. Australia's CDR, for instance, includes within its scope individuals, as well as small businesses.

Data portability can enhance competition in several ways. First, it can reduce information asymmetries between the providers of goods and services and their customers. Second, it can limit switching costs, including by reducing transaction costs. Third, it could reduce barriers to market entry, especially where data portability can provide access to critical data and reduce network effects.

This is best illustrated in open banking regulations such as PSD2 in the European Union. Open banking encourages banks to provide their customers' account information to certain third-party service providers. PSD2 introduced Payment Initiation Services and Account Information Services as a new category of service provider; bank account data are essential data for these services. Quantitative evidence on the overall impacts of data portability on competition is still limited. However, studies of the effects of the Current Account Switch Services initiative in the United Kingdom[13] show that it resulted in a 22% increase in switches compared to the predecessor system (FCA, 2015[50]). Also, after the Retail Banking Market Investigation Order 2017[14] and the Payment Services Regulations 2017 were introduced, more than 140 third parties registered for the scheme in the United Kingdom (Open Banking Limited, n.d.[51]).

Risks of unintended adverse effects on market structures

While data portability may foster competition through reduced switching costs, some factors may make the effects of data portability on competition less visible. Multi-homing and complementary services from other

providers (e.g. apps on Android provided by other entities than Google), for example, may reduce customers' interest in switching services, or their ability to switch, even if their data are portable. According to CERRE (2020[25]), the right to data portability is likely to benefit only the "old" customers of the incumbent; the "new" customers of a competitor entering the market (the entrant) are likely to be worse off. The authors argue this is because data portability strengthens the entrant's competitive position. As a result, it has fewer incentives to innovate to attract customers (see next section on "Stimulating data-driven innovation and unintended adverse effects on the incentives to invest"). This, however, assumes a correlation between data portability and the entrant's incentives to innovate and consumer surplus, for which there is not much evidence. Some studies show that when high switching costs and network effects co-exist in the market, lowering switching costs might or might not lead to pro-competition effects. Its outcome depends on other factors such as the maturity of industry (Chen, 2016[52]; Suleymanova and Wey, 2011[53]).

Also, data portability may favour incumbents that can better leverage their network effects thanks to data portability, which in turn would reduce possible positive effects on competition. That is, data portability may make it easier for consumers to switch to the incumbent or dominant competitor. Data portability, for example, could facilitate the incumbent's access to data in niche markets that are typically served by start-ups and smaller businesses:

> Markets with strong network effects tend to monopolise, because consumers tend to gravitate to the service or platform that already exhibits the largest network effects… Switching costs can dampen this process, because they create an economic friction (transaction cost) that prevents customers from switching to the service with higher network effects as easily. *(Krämer, Senellart and Streel, 2020[25])*

Finally, data portability requirements may not imply that digital services are interoperable and compatible. Data portability – in the case of the GDPR, for instance – gives data subjects the right to receive the data provided in a structured, commonly used and machine-readable format and to transmit those data to another controller. However, this does not mean the data can be transferred in a format that other systems can re-use. Interoperability was the goal of the right to data portability of the GDPR. However, controllers are not obliged to adopt or maintain processing systems that are technically compatible (European Union, 2016[54]; De Hert et al., 2018[55]). Anecdotal evidence confirms that even though many digital services enable consumers to download their personal data, they still rarely allow them to upload data from other services.

Universal requirements to interoperate with all other services would be expensive with uncertain benefits for most users. They might also disproportionately burden start-ups and SMEs, which would have to enter the market with systems to interoperate with all other systems already on the market. Conversely, dominant market participants would be more likely to have the capital to invest in necessary systems, as well as to play a role in determining standards. Cases where all competing services would need common features and functions could even result in less variety and feature competition in the marketplace. This, in turn, would reduce consumer choice and innovation. In addition, universal requirements to interoperate with all other services would raise concerns related to intellectual property rights (IPRs). This is especially the case when IPRs protect the data to be ported or the standards and APIs to be used (Rosschke and Zach, 2020[56]) (see also section below on interoperable specifications, including standards and APIs).

To minimise competition risks, stricter obligations on firms that process larger amounts of data, control sensitive data or are dominant in a particular market have been proposed. The Online Expert Consultation suggested that competition authorities may be able to integrate data portability into competition assessments. Data protection authorities could then clarify the scope and limits of data portability to increase certainty. These possibilities have not yet been fully explored. To address competition risks related to network effects and ensure that data portability promotes competition and innovation, CERRE suggests that enough users would have to consent to a transfer of their data. Further, data portability would

have to occur through continuously transfer of data through standardised APIs (Krämer, Senellart and Streel, 2020[25]). Under most current data portability regimes, this seems unlikely.

Stimulating data-driven innovation and unintended adverse effects on the incentives to invest

Opportunities for new or significantly improved products and markets

An important question is whether, in addition to fostering competition, data portability may also stimulate innovation. This could take the form of new products and services, expansion of existing markets or creation of secondary markets.

With respect to innovation, data portability is expected to help overcome the "cold start problem". This is based on difficulties faced by new digital product or service entrants to draw high quality inferences for its users due to lack of data (Kerber, 2019[57]; Krämer, Senellart and Streel, 2020[25]). It therefore can be argued that innovation activities would be significantly increased if new entrants could obtain data through data portability regimes.

For example, the UK's midata initiative allows people to download their current account transactions in a standardised format for easy comparison against accounts offered by other providers. According to the midata impact assessment, the programme anticipated that the release of transaction data would stimulate innovation and expansion of third-party choice engines such as price comparison websites. The midata consultation also highlighted other potential spin-off services, such as the loyalty-based service offered by a leading Finnish grocery retailer and third party. The service offered to inform customers of the nutritional content of their shopping basket based on data aggregated through loyalty cards. Since then, the UK government has taken steps to implement midata in the energy sector (BEIS, 2018[58]).

In addition, data portability could also stimulate the creation of new business models, including data intermediaries. Personal information management systems (PIMS) and personal data stores (PDS), for example, give more control to data subjects (consumers) over their personal data. In so doing, they restore user agency, including in the context of the Internet of Things (Urquhart, Sailaja and Mcauley, 2017[59]). By assessing and confirming the reliability and trustworthiness of data users, the PIMS/PDS can increase trust in data re-use and thus can function as an "Information Trust Bank". In Japan, for example, a PIMS/PDS application in tourism called *Omotenashi* collects personal information from social network services, which could be shared with local businesses (provided user consent is given) (OECD, 2019[9]).

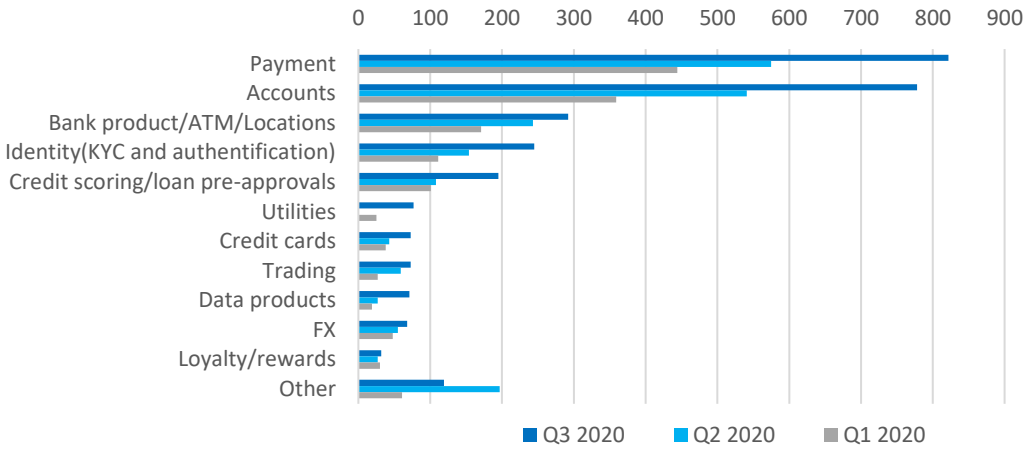
Data portability in the financial sector (through open banking and PSD2, for example) can also encourage unbundling and innovative re-bundling of financial services. This allows for the entry of new financial service providers and platforms. APIs in financial products make it easier for fintech firms to mediate contracts and transactions that traditionally only involve incumbent banks and their customers (LifeSREDA, 2016[60]). An Axway study shows that use of open APIs in the financial sector has enabled the market entry of fintechs and certain partnerships between fintech firms and traditional financial institutions (Axway, 2020[61]). For example, through banking-as-a-service – an API-enabled business model – banks provide core functionalities through a banking platform. This enables participating fintechs to build their own customer-facing banking offerings (Axway, 2020[61]). The report shows the number of banking platforms has grown significantly, particularly in the United Kingdom. This growth is apparently the result of data portability and API adoption. As another example, an API-enabled banking platform in Germany known as Fidor provides banks and fintechs with application modules for digital banking. These include communication platforms for interacting with customers, customer loyalty programmes and credit scoring (LifeSREDA, 2016[60]).

The Axway report is in line with findings showing the overall number of bank API products is increasing as a result of open banking regulations. Most of these APIs are for data that must be shared according to the

regulation. However, other data are also increasingly shared through APIs (Figure 4). The top two API products are "payment" and "account", which enable payments integration and review of account balances, respectively. A survey by Platformable shows the number of APIs for other data items has increased as well (Mathur, Boyd and Pham, 1 June 2020[62]; Pham, Boyd and Mathur, 13 August 2020[63]; Platformable, 2020[64]).

As in the financial sector, the use of energy consumption data diversifies the value-added data-driven services, as well as the web of partnerships in the value chain. Those data-driven services, which are often called "Energy as a Service", include advisory services based on customers' energy consumption, installation of energy assets such as batteries and energy-efficient appliances, and energy management services through monitoring, remote control and optimisation of energy use (IRENA, 2020[65]). In the United Kingdom, for example, second generation smart meters, which enable the transfer of energy consumption data, are associated with the development of data-driven services such as energy efficiency advice service and automation to enable demand-side response (BEIS, 2018[66]).

Figure 4. Bank API products by functionality/product categories Q1-Q3 2020



Note: "Utilities" is not represented in Q2 2020 survey result. Larger numbers of "other" in Q2 2020 may be the result of integrating "Utilities" into "Other" in that period.
Source: (Mathur, Boyd and Pham, 1 June 2020[62]; Pham, Boyd and Mathur, 13 August 2020[63]; Platformable, 2020[64]).

Risks of unintended adverse effects on incentives to invest

Data portability can also have adverse effects on innovation for market participants in certain situations. One possible negative effect is the risk of losing the user base due to lower switching costs. This could result in a disincentive to invest and innovate in the first place given the lower expected returns on investments (see point above). In addition, incentives to invest in data and innovate may be reduced as data management costs tend to increase with data portability. Higher digital security and privacy risks can also reduce incentives. These higher costs, in turn, can reduce returns on investments. Disincentives to invest and innovate may also result in cases where the portability of certain types of data (e.g. inferred or derived data) become mandatory (see section below on the risks of anti-competitive effects).

Swire and Lagos (2013[67]) argue the data portability requirement in the GDPR may put start-ups and SMEs under the obligation and handicap of having to invest in data portability.[15] These authors concluded that where businesses build their competitive advantage based on user and data lock-in, data portability could undermine incentives to invest in data in the first place. For some start-ups, this could mean they lose their attractiveness as acquisition targets of larger firms, and thus part of their economic value.

Another major risk is related to the growing empirical evidence that some firms may have established "kill zones" around their core business model. CERRE (2020[25]) describes this phenomenon: "innovative start-ups, which may become competitors to a big tech firm's data-centric business model [due to data portability], may either be bought by the big tech firm, or it is quick to incorporate the innovation into its own service". As a result, the chances for a disruptive business to successfully challenge the core business model of a big tech firm is rather low. This, combined with the above, implies that the positive effects of data portability on innovation, under these circumstances, may be limited to complementary and new digital markets. This is in line with a report by law firm White & Case (2018[68]) that open banking has stimulated mergers and acquisition activity (see also Open Banking Expo, 2018[66]).

Facilitating data flows and data sharing, and their digital security and privacy risks

Opportunities on enhancing access to and sharing of data

Data portability could facilitate data flows and increase users' trust and empowerment in the digital economy, thereby increasing their willingness to provide more data. Data portability may also help overcome existing barriers to personal data sharing, including across borders. Individuals theoretically have more control over their personal data and may effectively decide how and to whom their personal data are transferred. This, in turn, may result in improved goods and services available to consumers, including via trade.[16] Such an outcome may arise especially when the services provided are substitutes and one of the service providers has an incentive for anti-competitive behaviour.

To this end, the Centre for Economics and Business Research has suggested that data portability in the banking sector would improve the availability of customer information to banks. This could enable creation of better risk profiles, allowing banks to offer more accurate interest rates depending on these profiles (Trustpilot, 2018[69]). The study estimates data portability enabled by open banking would result in a 7% reduction in the credit spread (risk premium add-on to the risk-free rate) on mortgages, totalling GBP 1.069 billion. Based on this result, the economic impact of "data mobility" is estimated at GBP 27.8 billion across the sectors (Ctrl-Shift, 2018[70]).

Digital security and privacy risks, including risk of personal data breaches

Facilitating data flows and data sharing through data portability comes with significant digital security and privacy risks, including the risk of personal data breaches.[17]

In respect to digital security risks, data portability typically requires opening information systems so legitimate users (or third parties on their behalf) can access and share data. This may, however, increase the risk of data breaches, even where strong digital security measures are implemented through secured APIs: the more accessible an individual's personal data, the greater the risk that information could be accessed and shared inappropriately by a third party. In addition, data portability may also further expose potential vulnerabilities of an organisation's information systems to digital security threats. This, in turn, can lead to incidents that disrupt the *availability*, *integrity* or *confidentiality* of business critical data and information systems. Much depends on the identification, authentication and other security measures of companies to respond to data portability requests and to manage related digital security risks.

In terms of privacy risks, at least three related challenges must be addressed. First, giving data subjects the ability to have their personal data ported on request from one data controller to another may increase the risk of identity fraud. Processes in place to confirm the identity of data subjects requesting their data be ported need to be sufficiently rigorous but simultaneously allow for data to be ported without undue hindrance.

Second, requiring data portability may undo some of the "privacy by design" efforts of private actors to protect privacy. This is especially the case if it is unclear to what extent processes to automatically de-identify users' data may have to be scaled back so that personal data can be identified and ported.

Third, as discussed further below, data portability may infringe the privacy of third parties with a stake in the data that are being ported from one controller to another. For example, a user that seeks to port a group photo or their contact list is necessarily asking to port data that involves the personal information of third parties (namely the other people in the photo and the people in the user's contact list). Although those third parties may have consented to their information being available on one platform, they have not necessarily consented to it being copied and made available elsewhere.

These privacy risks are exacerbated because data are being ported or transferred from one context to another. This change of context can make it particularly challenging to ensure that rights and obligations are not (accidentally or deliberately) undermined. This might happen, for instance, when privacy assumptions implicit in initial usage no longer apply in subsequent uses.[18] This raises a number of regulatory and implementation challenges. Questions about privacy, especially related to health care and social network data, are the most pressing. For example, in its investigation into Flo Health, Inc. (a fertility app), the United States Federal Trade Commission (FTC) assessed the privacy risks that may arise when consumers input health data to a non-HIPAA-covered entity, among other issues.[19]

To establish trust and ensure the protection of data, including privacy and personal data protection, countries implementing a data portability regime must have a robust privacy framework. It must apply to ported data, with remedies for breach and an oversight body, and clear liability assignments. The implications for privacy and digital security, and the responsibility and liability challenges, are discussed in more details in the next section.

Achieving "informational self-determination" and the risk of over-collection of data

Opportunities resulting from greater control and agency over data

As mentioned above, data portability may help address the power imbalance between consumers and digital service providers. In so doing, it can empower data subjects through an easier exercise of their right of participation under applicable legislation (i.e. to ask an organisation to verify if it has information about them).[20] Specifically, the ability of a data subject to download personal data that a data controller has collected about them increases transparency. It allows data subjects to determine whether they consider further action (like correction or deletion) to be necessary.

In addition, the ability to transfer personal data between data controllers can help individuals move from a data controller with poor privacy and data management capabilities to one with policies and practices that better align with their expectations. Data portability may also protect against loss or unavailability of personal data should a provider go out of business. An individual would be able to request transfer to a new provider, rather than losing their customer history and having to start fresh. All this contributes to users' informational self-determination.

Risks of violating the collection limitation and the purpose specification principles

Despite the possible benefits, the potential of data portability to help achieve informational self-determination is not always assured. The benefits of empowerment may be conditional on the extent to which data portability can be effectively and securely implemented. For example, the data transfer may not be secure enough or data subjects may not be aware of how the new data controller could protect their personal data and privacy. More importantly, there could be strong switching barriers such as users' multi-homing on complementary services, direct and indirect network effects, and users' behavioural inertia.

Furthermore, there is a risk that data portability could facilitate over-collection and over-sharing of data with new service providers (including comparison services). As highlighted above, data portability is a means for data collection. Some have raised concerns that consumers could be pressured to provide their data to other additional data holders, which could be used against their interests. An often presented example is the possible request of an insurance company to a consumer to transmit its social network data as a condition for contracting. This propensity of certain service providers to collect and ask for more data as a condition for contracting could also lead to a re-intermediation of personal data controllers. Gal and Rubinfeld (2019[44]) warn "the easier it is to share data, the greater the concern that private data will fall into more hands." Further, MacCarthy (2020[71]) argues that "[u]sers who trust their information with one online company might not be pleased to share their sensitive data with any and all potential rivals." In this context, it is therefore critical to underline the obligation of data users to minimise data use, and the importance in the choice of data formats that can affect data minimisation.

Conferring on individuals a right of data portability arguably affects organisations' ownership and control over the data they collect. Indeed, one of the main rationales for data portability is to reduce lock-in and increase competition by facilitating data sharing in accordance with users' preferences. However, this raises certain questions. What are the obligations of data controllers to ensure recipients have adequate data management and security and privacy processes? When, if ever, are data controllers liable for recipients' mishandling of data (particularly when controllers were just complying with a data subject's request for data porting)? Will organisations be less incentivised to robustly manage data security risks if they feel they have lost ownership or control of it? How does data portability affect organisations' and users' ownership of data? These implementation challenges are addressed in the next section.

Implementation challenges to be addressed

The task of regulating data portability involves balancing various competing policy tensions. Such tensions include fostering competition and innovation but protecting privacy, IPRs and incentives to invest; enabling data sharing among competitors but ensuring the security and privacy of user data and avoiding anti-competitive information sharing; and enhancing interoperability but not hampering innovation and excluding new entrants by mandating unnecessarily stringent standards. Regulators must consider how data portability aligns with frameworks related to cross-border data flows, privacy protection, accountability and compliance, enforcement and many other issues. Stakeholders engage in such balancing exercises to assist policy makers, regulators and others. The following section analyses some of the main challenges to avoid unintended consequences if these tensions are not fully appreciated.

Addressing the implementation challenges in this section is also critical to further promote adoption of data portability. Adoption of data portability remains low because of legal uncertainties regarding the scope of data portability, poor interoperability, digital security and privacy risks, and liability challenges. Other reasons for low adoption are the still low level of awareness of consumers about their right to data portability. This was highlighted by experts during the Online Expert Consultations but also by the OECD Online Platform Survey in 2020.[21]

Responses from the Online Platform Survey suggest that platforms have taken steps to self-regulate. They may intend to inform the content and scope of data portability guidelines and requirements enacted by regulators. However, they still face a number of challenges when implementing data portability. As many online platforms depend on their user base, most (prior to the formalisation of the right to data portability) stored and kept users' data so they could not be extracted by the user or more importantly by a potential competitor (Graef, Wahyuningtyas and Valcke, 2015[72]; Engels, 2016[73]). As a consequence, the main concern derived from the lack of data portability, was (and often still is) that users had to face the subsequent risk of lock-in and high switching costs. This occurred because many businesses aimed for a competitive advantage by exclusively collecting and processing users' data (Engels, 2016[73]). By keeping

their systems closed, online platforms also caused access problems for other platforms that required user data to provide complementary or competing services and products (Engels, 2016[73]).

Nevertheless, even before several jurisdictions formalised data portability in legislation, numerous online platforms recognised that it responded to an increased desire from users (both individuals and organisations) to control and, where requested, to share and re-use data about them across online platforms. In particular, data portability can help users counter the above-mentioned lock-in effects and to reduce switching costs, among other benefits. As several OECD countries have adapted legislation that formalised the right to data portability, an even larger number of online platforms have adopted initiatives to comply with such legislation.

Uncertainties regarding the scope of data portability

The significant differences across data portability initiatives have created uncertainty for market participants and users. Significant differences of such initiatives relate to their purpose, scope (who has the right to have data ported, what data can be ported, whose data should be portable), exceptions to mandatory porting and possible consequences for non-compliance. The issue of scope may also consider whose data should be portable (especially given that data are often associated with more than one person such as in the case of e-mails, pictures or videos). It is an implementation challenge for data holders to account for each individual's rights.

Responses from the Online Platform Survey confirm the importance of this challenge. In particular, online platforms indicated that legal requirements on data portability were unclear, overly complex and sometimes frequently changing. Respondents noted numerous related implementation challenges for online platforms, including identifying which data sets should be made available for data portability. To this end, there is some uncertainty among platforms regarding whose data should be portable. This is especially the case where data are associated with more than one person (see section below).

Uncertainties with respect to observed data

There is a consensus among practitioners, regulators and policy makers that *volunteered* data should be subject to the right to data portability while inferred and purchased data should not. However, uncertainties remain on whether observed data should be subject to portability rights. For instance, the right to data portability under the GDPR (Art. 20) regulates personal data provided by the data subject to a data controller. The article has raised questions about what it means for a person to port the data they have "provided" to a service. According to the (former) Article 29 Working Party (OECD, 2015[34]), the right to data portability under the GDPR would include both volunteered and observed data. It would, however, exclude data derived (inferred) from additional processing that are often considered proprietary.

Including volunteered data within the scope of data portability reflects the paramount contribution of users (data subjects) in the creation of the data and therefore their legitimate interests in being granted full access and use rights to the data. Along the same lines, excluding inferred data from the scope of data portability also reflects the paramount contribution of the data holder (data controller) in the creation of that data (which is primarily enabled thanks to proprietary algorithms and analytical processes). In other words, including volunteered and excluding inferred data is proportionate to the respective contributions of users and data holders in the creation of the data. It would therefore seem coherent to include certain types of observed data. However, this would depend on the degree to which users and data holders have contributed to their creation. For example, observed data that are immediately processed and enhanced to generate inferred data would no longer have to be provided via data portability. This is in line with Ruth (2017[74]), who argues that observed data should be considered as "provided" by the data subject according to Art. 20 GDPR under two conditions. It would be "provided" whenever the data subject willingly contributed to the acquisition of such data *and* the controller did not add any value to the data besides

storage. Ruth (2017[74]) also notes it seems prudent to make the right to data portability subject to a proportionality requirement.

Uncertainties with respect to data relating to third parties

The issue of scope also includes questions as to whose data should be portable given that data are often associated with more than one person. This is the case, for example, with digital images (photos, videos) and e-mails. Ensuring each individual's rights are accounted for is therefore a major implementation challenge for data holders.

When individuals opt to download their data from a data controller or request the data be shared with a different controller, the first controller must determine (within the parameters set by the law and regulatory guidance) what constitutes the requesting party's personal data and where they implicate or become someone else's. For example, is Platform X able to share the text of a conversation between User A and User B with Platform Y at User A's request, or would that breach User B's privacy? Is Platform X permitted to share a group photograph with Platform Y at one person's request, or does that infringe the privacy of all other individuals in the photograph if they have not consented? The UK Information Commissioner Office's guidance note on data portability provides that a new controller that receives data should assess whether the data contain any third-party data. If they do, the new controller must assess whether it has a lawful basis for processing those data. If not, it should delete those data as soon as possible (United Kingdom ICO, 2019[75]).

It is possible to share only one side of a conversation or a cropped image. However, those data are likely to be considerably less useful to the recipient, obviating the advantage of increased competition from data portability. The incomplete data may be ambiguous and, at worst, misleading. This in itself comes into conflict with data governance laws that require personal data to be accurate and complete (see, for example, OECD Privacy Guidelines, Principle 8). Good practice may require the porting organisation to fix any issues with the ported data (e.g. incomplete or corrupted data) within a specified timeframe.

At both the OECD Expert Discussion on Data Portability and the OECD Workshop on Data Portability, experts confirmed that data portability was challenging when multiple actors hold different and overlapping interests in relation to the same data (see also FTC, 2020[46]). Those interests include data protection, innovation, competition, IPRs, contractual rights and confidentiality. However, experts also stressed that conflicting rights did not necessarily mean that data cannot be ported. Rather, any balancing of competing interests should be done transparently and with separate oversight over how decisions are made.

Digital security and privacy risks

Advances in technology and changes in organisational practices have transformed occasional transborder transfers of personal data into a continuous, multipoint global flow (OECD, 2011[76]). Although this has brought associated economic and social benefits, it is increasingly difficult for individuals to understand how their personal data are collected, processed and used. Advances in analytics also mean that an increasing quantity of data can be related to an individual, prompting heightened privacy-related concerns (OECD, 2011[76]). Yet another implication is increased risk of data breaches, including as a result of accidents, malicious hacking, unauthorised access or disclosure, phishing and denial-of-service attacks. Such breaches represent more than a privacy violation of the individuals whose personal data have been breached. They can also cause significant economic losses to the business affected, including loss of competitiveness and reputation. Further consumer detriment may also result from a data breach, such as harm caused by identity theft.

Recent statistics demonstrate that public perception and awareness of the importance of privacy and data security are changing. For example, in 2019, Eurostat assessed security views of individuals within the European Union who used the Internet within the past year. Half of the individuals said that security

concerns limited or prevented them from doing certain online activities. Examples of activities included Internet banking, buying goods or services on line, downloading files, communicating with public services or administration, or using the Internet through public WiFi (Eurostat, 2019[42]). In the United States, a study indicated that 81% of Americans believe the potential risks of data collection by companies outweigh the benefits (Auxier et al., 2019[77]). In Australia, a government survey revealed that 69% of Australians were more concerned about their privacy in 2017 than in 2012. Furthermore, most Australians were concerned about their privacy in the digital environment (OAIC, 2017[78]).

A data portability regime may heighten these issues and concerns. In other words, freeing up the transfer of personal data between organisations on data subjects' requests may increase personal data flows; confuse individuals' conception of how their data are collected, processed and used; and, in some cases, prompt them to limit or refrain from certain activities on line. Accordingly, trust in any data portability regime should be fostered so the potential benefits of portability are realised. Fostering trust in the regime and in organisations' commitment to personal data security and privacy is likely to be key to individuals taking advantage of any portability right.

There are at least four preliminary observations regarding implementation (see section above on the "opportunities of data portability and their associated risks" for more general observations on the privacy and digital security risks). First, data portability initiatives should clearly delineate where liability falls in the event of a privacy violation, including a data breach. Effective portability frameworks may hold participants liable for their own conduct, but not the conduct of other participants, in accordance with existing legal frameworks. This will likely require attention at a national level in accordance with laws governing liability.

Second, there is a strong probability that data portability initiatives may span multiple regulators.[22] Governments implementing data portability schemes, therefore, should be wary of this likelihood. Consequently, they should plan which regulator will have primary oversight of the initiative to ensure efficiency, streamlined processes and beneficial consumer outcomes.

Third, data controllers may be able to help with enforcement and simultaneously contribute to the building of such trust, particularly if paired with effective oversight by regulatory bodies and enforcement. In data protection and privacy communities, the concept of accountability has evolved from simple compliance with legal obligations. Today, it refers to proactive efforts by companies to show regulators and the public how they integrate privacy by design principles into their goods and services. In the data portability context, the transparency in such proactive accountability can help regulators quickly understand the privacy and security protections in place for data that are being ported.

Fourth, to exercise their rights to data portability, users must prove their identity and their legitimacy to initiate and receive the data to be ported. This is critical because as Swire and Lagos (2013[67]) highlighted, data portability can pose serious risks to privacy and data protection. They point out that "when an individual's lifetime of data must be exported 'without hindrance', the one moment of identity fraud can turn into a lifetime breach of personal data" (see also next section on digital security). Digital identity management and authentication measures therefore become essential, but their use may also raise questions. To what extent could the further collection of personal information to ensure proper authentication in itself pose a risk to privacy? Ideally, digital identity management and authentication measures would need to vary depending on the nature of the request, the sensitivity of the information communicated and the context in which the request is made. This is in line with the general opinion that additional collection of personal data should not be systematic, and only necessary when the identity of users is in doubt.[23]

Responses[24] from the Online Platform Survey confirm these challenges. However, they also indicate that platforms have taken measures to minimise digital security and privacy risks related to data portability, notably:

- *Account authentication*: Users have to re-authenticate their account to execute a download, even if they already signed in. This process encompasses a two-factor authentication and other security prompts when an account is especially vulnerable or the download is initiated from a new computer.
- *Encryption:* The data are encrypted in transit to the user's device or to a third-party destination.
- *User notification:* Users are notified when data exports start and conclude. Pre-export notifications are delivered to users via multiple methods to ensure they are notified that someone is exporting their data even if their primary account is "hijacked".
- *Delayed takeout delivery:* For certain users, the delivery of exported data is delayed to help mitigate a situation where an unauthorised individual has accessed a user's account and attempted to access or save a copy of their data.
- *Archive expiration:* The archive data are only available for a limited amount of time period, after which the account has to be re-verified and the data re-exported.
- *Transferring service's access:* A transferring service's access to the destination service could end once the transfer of data is complete.

Digital security

Security of personal data must be ensured by the original data controller, the receiving data controller and any intermediaries involved in the transfer process. All parties must have adequate security measures in place to ensure the integrity and security of the data and the privacy of data subjects.

A comprehensive risk management approach may help mitigate data breach risks, balance trade-offs and promote data access and sharing, including across borders. The objective of such an approach is not to eliminate risk; rather, it is to "increase the likelihood of economic and social benefits from the data value cycle by minimising potential adverse effects of uncertainty related to the availability, integrity and confidentiality of the cycle" (OECD, 2015, pp. 211-12[34]). However, a risk management approach remains challenging to implement for most organisations, including SMEs. The OECD highlighted EASD challenges in its 2019 report (OECD, 2019, pp. 85-87[9]).

For instance, is the original data holder that transfers the data (a transferor) obliged to ensure the data recipient has adequate security measures to protect the data it receives? If the recipient lacks these measures, should the transferor bear some liability for any resultant damages? These remain open questions. Countries have various mechanisms to ensure that data recipients are sophisticated enough in their data governance practices to ensure the security of the data they receive. Australia's CDR, for example, is premised on the notion that data may only be ported to certified entities (ADRs). Accreditation may be granted based on compliance with various requirements set by the regulator. These requirements make it easier for customers to determine which data recipients adopt trustworthy security practices. This system also means the transferor need not be concerned by the digital security systems in place in the ADRs. This system is designed to facilitate efficiency and trust whereas the former system put the onus on banks to independently approve entities before entering into data sharing arrangements (Australian Government, Department of Treasury, 2017, pp. 22-23[79]). Australia's system drew upon PSD2 (which develops a publicly accessible central register of authorised payment institutions) and the UK's Open Banking model (where third parties must demonstrate the effectiveness of their processes to protect sensitive payment data) (Australian Government, Department of Treasury, 2017, p. 24[79]). These jurisdictions also have sophisticated data protection and privacy regimes that apply to controllers processing personal data of their citizens.

The security of data *during* a transfer, and associated allocation of responsibility and liability, must also be factored into any data portability regime. Of relevance here are APIs and standards for data encryption. Another way of potentially mitigating security concerns with data portability is the introduction, maintenance and enforcement of robust technical standards, including for data encryption, that apply to all participants.

Some countries are already engaged in such work. The Information Commissioner's Office (ICO) of the United Kingdom, for example, has released simple and detailed guidance notes for organisations regarding encryption in transit and at rest.[25] Similar guidance has also been published by the European Union Agency for Network and Information Security (such as on recommended cryptographic methods), the FTC of the United States (FTC, 2015[80]) and the United States National Institute of Standards and Technology (such as Special Publication 800-131A Revision 1), among others.

Privacy and personal data protection

Data portability in this paper is restricted to the transfer of data when they are *requested* by a data subject. Such requests can be seen as an implicit consent by the data subject to transfer data. However, explicit consent may be necessary to ensure the privacy of data subjects is protected. Consent can be manifested in different ways. Best practices might dictate that, before data are ported, the consent of the data subject be i) specific, as to when data are ported, what data are ported and for how long; ii) informed, as to what data are ported and what the recipient will and may do with the data once received; iii) explicit, as opposed to implied from past behaviour or general use of a service; iv) time-limited, such that the data holder knows the length of time within which data may be shared and whether the data flow is continuous; and v) easily revocable with immediate effect, such that the porting of data may be stopped at any time.

Good practice may also dictate that data subjects requesting data portability be informed or reminded that data portability is distinct from the right (in some jurisdictions) to be forgotten. Moreover, they should be aware that an act of porting data from one controller to another does not allow the first controller to unilaterally erase the subject's data from its systems. In other words, the right to data portability is different to the right to request erasure of one's data. While the two requests may be made at the same time, a data subject must be astute or informed enough to recognise the difference and the need to exercise both rights.[26]

Other good practices exist to ensure the privacy of the requesting party in a data portability scheme. For example, all parties handling data should be subject to a robust privacy framework that adopts and enforces, at a minimum, the basic principles set out in the OECD Privacy Guidelines (OECD, 2013[3]). Such a framework will constrain the ways in which data recipients may process and use the data they receive, such as limiting them to the purposes specified in the portability request. Best practice may also require participants in a data portability scheme to adopt privacy-enhancing technologies where appropriate. For example, they might adopt a scheme when data are encrypted or when data are anonymised before being transferred (see Box 3). The latter can be particularly critical where data belong to more than one data subject, such as transaction data of a joint bank account or a picture of multiple individuals. In these cases, it may be possible and appropriate to anonymise the information belonging to third parties if receiving authorisations for data transfers from all third parties is not possible.[27]

Furthermore, a record of data transfers (so data subjects can see their portability requests and interactions), combined with formal complaint and dispute resolution processes, are also good practices to ensure effective privacy and data protection.

Box 3. Privacy-enhancing technologies

Privacy-enhancing technologies (PETs), such as anonymisation and cryptography technologies and techniques, are increasingly viewed as promising approaches to prevent and mitigate the risk of privacy and confidentiality breaches and enable organisations to better manage data responsibly. PETs thus make it possible to balance the respective interests of data users and data subjects by enabling data access and use, while data subjects' privacy remains protected.

PETs typically help reduce the risk of privacy and confidentiality breaches by minimising information disclosure in a number of ways. Some PETs seek to curb "default" data disclosures; that is, they are designed to prevent any disclosure of data, unless strictly necessary to provide the envisaged functionality. In this case, PETs primarily aim to minimise the risk of inadvertent disclosures (e.g. due to how a specific system operates). A commonly used application of this type of PETs is the Internet security protocol Transport Layer Security (TLS). This is used by Internet browsers, mobile applications (apps) and web servers, among others, to exchange sensitive information such as passwords and credit card numbers. TLS is commonly used for data portability downloads and transfers (OECD, 2017[81]). Other PETs do not focus on data minimisation, but rather on *obfuscation* with the goal to introduce "noise" and thus prevent data collection.

Responsibility and liability challenges

Data controllers and recipients require clarity and certainty about their responsibilities to engage with data portability regimes. This includes activities such as responding to requests and transferring and receiving data, and how those responsibilities result in exposure to liability (Egan, 2020[82]; IIF, 2018[83]). Generally, the liability risks associated with data portability relate to digital security breaches and privacy violations (as discussed above). However, they may also relate to damages arising from other types of incidents (e.g. poor data quality). How and what types of risks arise depend significantly on the industry context and the data portability model. For example, were the data provided to the data subject, to an intermediary or directly to the recipient data controller? Were the data provided on a one-off basis or via a live feed or API?

Responses[28] from the Online Platform Survey confirm that online platforms face liability challenges; some expressed concerns regarding lack of clarity in this area. Some suggested the responsibility of online platforms with respect to those individuals whose interests might be implicated by a data transfer could be further clarified. In addition, one platform suggested it was also unclear whether and to what extent the original data holders would remain liable for data misuses or the poor implementation of safeguards by the receiving data holder chosen by the data subject.

Mechanisms for assigning liability

Data portability regimes contain a variety of mechanisms to assign liability for certain risks. Broadly speaking, liability is assigned in one of three ways: i) within the specific data portability regulation; ii) in general data protection frameworks; iii) or by contract between the participating parties. The Australian CDR legislation, for example, creates a number of criminal and civil offence provisions, including for making a false or fraudulent request or falsely holding out status as an accredited data intermediary. The legislation also immunises organisations from liability for contraventions of the CDR obligations if their conduct is in good faith and in compliance with the law.[29] By contrast, the GDPR does not contain specific provisions regarding liability risks. However, the (former) Article 29 Working Party provides general guidance as to how data controllers can comply with the Article 20 data portability right (and therefore avoid liability for non-compliance under the GDPR). However, the GDPR does not replace other, stricter frameworks regarding liability in certain contexts, such as payments.[30] If the regulations do not apportion sufficiently

clear liability, data entities may seek to include liability waivers in their contracts with data subjects and recipients in the case of transfers to the ultimate data recipient or a data intermediary.

One common approach considers the responsibilities of the entities and individuals involved in a data portability regime to inform placement of liability. Some broad principles can be identified, including that liability follows the data. In other words, the original data controller is responsible for ensuring the request is valid, including verifying the identity of the requesting party; responding to the request within the required time periods; collecting and collating the data within the scope of the data subject's request; and securing the data for transfer and effecting the transfer in accordance with the data subject's instructions and consent, including in terms of ensuring the correct recipient is identified. Some frameworks also require the original data controller to ensure the recipient is accredited to receive data under the data portability framework (e.g. Australian CDR). Others are clear that the original data controller does not have the responsibility to ensure the recipient data controller is compliant with relevant data protection laws (GDPR, as explained by the former Article 29 Working Party) (OECD, 2015[34]). Other approaches involve the use of trusted third parties that manage the contractual relationships between a controller and third-party data re-users to frame their respective responsibilities and liabilities. The data connect initiative of Enedis, a French company, provides one example. Enedis took advantage of its data portability obligation on its smart meter data to develop a platform that controlled data portability from end to end – in terms of digital security, liability and information delivered to the user (see also section further below on the role of trusted third parties in reducing transaction and compliance costs).

The original data controller has the most significant engagement with the data subject. Consequently, it is expected to provide clear information to the data subject about the terms and conditions and risks of transfer. This would ensure that consent of the data subject is clear and informed. To reduce its risk in relation to the scope and content of the data being transferred, the original data controller can involve the data subject in identifying, selecting and reviewing the data to be ported (OECD, 2015[34]). Explicit and informed consent are essential to initiating a data transfer. However, data controllers would likely still be held liable if data were transferred incorrectly or outside the scope of the consent, or for any security or corruption issues relating to the transfer.

Liability after the data transfer

Once data are received by the data user, intermediary or recipient data controller, the original data controller's responsibility for the security and quality of the data is assumed displaced. The exception to this rule relate to any issues that are clearly the fault of the original data controller (e.g. transferring an incomplete, corrupted or unsecured file, or sending data to the incorrect recipient). This liability can be reflected in regulation and confirmed in the consent contract between the data controller and data subject. For example, under the proposed Singaporean data portability regime, original data controllers would be required only to "check that the data transmitted has been received by the receiving organization and assist with any queries it may have with respect to the data transmitted". Further, the Australian CDR regimes obliges the recipient data controller and/or data intermediary to guard against any misuse, interference, loss or unauthorised access, modification or disclosure.[31] In this context, once the recipient data controller receives the data, it is responsible for compliance with any requirements in relation to processing the data. In addition, it must ensure the data received are correct and appropriate for use. If the data received contain third-party data, the recipient would also be prevented from using or processing the data without the consents required by the data protection laws. This is the case even though the original data controller may have had those consents at the time of transfer.

Under the above frameworks, the original data controller would not be held liable for any claims for damage resulting from processing (lawful or otherwise), use, misuse or subsequent transfer by the recipient data subject or data controller or the data subject. This framework also reflects the fact that the data subject chooses the recipient. Therefore, data subjects must ensure they consent to the terms and conditions and

privacy policy of the recipient data controller. That said, the recipient data controller may act inconsistently with the terms of the data subject's consent for data transfer to the recipient. In these cases, the data subject may have a right of action against the recipient data controller under ordinary legal mechanisms. This further highlights the necessity of clear and comprehensive information being provided to the data subject before consenting to the data transfer (either at the point of making the request, or at a final approval stage). Nonetheless, there may be a role for regulation to clarify the relationships and obligations so that all parties are clear as to their responsibilities and potential liability.

Liability in respect to third parties

Aside from the above general principles relating to actors' responsibility, data controllers are expected to be aware of particular liability risks in some contexts. Some other risks for policy makers and data controllers to consider are the following:

- *IPR violations resulting from transfers, including where trade secrets and other similar rights (e.g. EU sui generis database rights) are implicated in the data subject's request.* In relation to IPR, the Article 29 Data Protection Working Party's Guidelines on the right to data portability clarify that data controllers cannot rely on risks to avoid complying with a portability request, such that the onus is on the data controller to comply with requests in a way that protects any business interests[32] (OECD, 2015[34]).
- *Instances where the data recipient relies upon incorrect or incomplete data received from the original data controller*. This risk can arise in a variety of situations. For example, the recipient data controller may deny a loan to a consumer based on inaccurate data from the original data controller. Further, liability questions arise in the context of technological repair and maintenance information in relation to a car. A service provider or repairer, for example, may fail to address an issue that results in an accident because the original equipment manufacturer provided incomplete data. In relation to data quality, the Working Party advises that "[d]ata controllers answering a data portability request have no specific obligation to check and verify the quality of the data before transmitting it." It also notes that data controllers remain subject to GDPR obligations to ensure the accuracy of personal data under their control (OECD, 2015[34]).[33] The Australian CDR legislation takes a more explicit approach, requiring the data holder to take reasonable steps to ensure the data being transferred are accurate, up to date and complete.[34] In one scenario, a recipient data controller may receive incomplete or inaccurate data that it processes and relies upon to make decisions about the data subject. This could relate to offering certain health care or banking services or insurance premiums. If this happens, either the data subject or recipient data controller may have a right of action against the original data controller.

Effectiveness and enforcement

Apportionment of liability is necessary to ensure sufficient efforts are made to guarantee the security and efficacy of data portability regimes. However, it must also consider the burden placed on data controllers and recipients to avoid liability. This is especially the case for small business that may also be subject to data portability requests. If they prevent new entrants from engaging in industries where data portability regimes are effective, unduly burdensome requirements to avoid liability for security breaches may reduce the pro-competitive benefits of data portability regimes.

Further, liability discussions must also consider enforcement mechanisms. Data subjects, for example, could enforce liability. On the one hand, they could seek redress through private rights of action under regulatory mechanisms, private tort law or contract law. On the other, they could seek redress through criminal or civil penalty enforcement proceedings, as is the case under the Australian CDR legislation and rules. Additional consideration should also be given as to whether liability is strict liability. Is it subject to

questions of reasonableness and whether harm or injury is required for standing? If so, how is harm or injury defined and how can damages be calculated?

Ultimately, the enforcement and redress mechanisms are likely to vary depending on the particular breach or contravention in question. For example, privacy-related breaches may be more appropriately addressed under general privacy laws (along with any data breach notification laws) than under the data portability framework. If the breach involves disclosure of competitively sensitive information or infringement of an IPR, liability could be determined and addressed in accordance with legal frameworks in the appropriate jurisdiction. Where liability is determined by contract between the parties rather than or in addition to regulation, the parties can consider whether any security measures, warranties or immunities are also appropriate.

Interoperable specifications including standards and APIs

Lack of common standards and interoperability is one of the most frequently cited barriers to the implementation of data portability and for effective re-use of the data. Users, in practice, may face difficulties porting their (personal) data because most information systems are not interoperable and standards are a condition for interoperability. These standards can exist at various levels corresponding to the aforementioned interoperability requirements for data, protocol, information systems and digital services. Even use of commonly used machine-readable formats may not guarantee data interoperability. As highlighted in OECD (2019[9]), and noted in previous sections, common formats may enable *syntactic* interoperability, i.e. the transfer of "data from a source system to a target system using data formats that can be decoded on the target system" (and thus accessibility). However, common formats do not guarantee *semantic* interoperability, defined as "transferring data to a target such that the meaning of the data model is understood". Both syntactic and semantic interoperability are needed for the re-use of data. Regarding this potential gap, the (former) Article 29 Data Protection Working Party (2017[84]) guidelines on data portability complement the requirement of machine-readable format with the intent to achieve interoperability. They explain that "[t]he most appropriate format will differ across sectors and adequate formats may already exist, but should always be chosen to achieve the purpose of being interpretable."[35]

Responses[36] from the Online Platform Survey underline the lack of standards and technical inconsistencies as major challenges in importing data from other online platforms. In particular, a major challenge was to ensure compatibility between data models. In this context, respondents highlighted the challenge of identifying common standards for data while balancing the need for new and innovative (as well as an increasing variety of) data formats with data interoperable formats and standards. Another related challenge was to provide data that are both machine-readable and intelligible to end-users, while managing the growing variety of technological, business and legal requirements.

Respondents noted that data formats were often specific to use cases even within a single category of data. In this regard, building common, open-source data models and data format standards was highlighted as a possible solution. These common standards should also guarantee privacy protection in data portability, one respondent noted. Another respondent indicated that other online platforms rarely made requests to import data. Nevertheless, this respondent pointed out that importing data while ensuring data minimisation and data quality was a great challenge.

Several respondents indicated their participation in the DTP as an example of co-ordination between online platforms on data portability (see Annex A). The project aims to create an open-source, service-to-service data portability platform to enable users to easily move their data between online service providers whenever desired. The project is a collaboration of organisations committed to building a common framework with an open-source code that can connect any two online platforms, enabling a seamless, direct, user initiated portability of data between the two providers.

Respondents also provided some recommendations for governments on data portability standards and technical requirements. In particular, respondents highlighted it was critical to consider the policy objectives to be achieved through the right to data portability. Depending on the priorities of these objectives, different standards, and technical and legal requirements for data portability could be appropriate. This is especially the case with respect to the scope of data to be ported and the liability frameworks associated with data portability obligations for service providers.

The importance of technical standards and interoperability for data portability

Gal and Rubinfeld (2019[44]) discuss the potential for competitive benefits and "data synergies" that can result from data standardisation in combination with data portability and data interoperability. Indeed, data standardisation enables smooth data flows, guarantees interoperability and increases competition and innovation. The authors find that without data standards, firms can be reluctant to share data, including due to increased costs. This can "result in the balkanization of data within particular sectors or even firms, thereby not only impeding innovation within markets, but also reducing spillovers to the improvement of analytical tools and to other markets" (Gal and Rubinfeld, 2019[44]).

At the Online Workshop, it was recognised that standardisation may help facilitate data portability and interoperability, particularly in industries that do not otherwise have incentives to facilitate data sharing. It was noted that industry participation in the creation of standards is key as it can create ownership of the standards and consequently help ensure widespread adoption and compliance. However, the discussion also noted that a preliminary focus on setting standards has delayed interoperability. Conversely, regimes that have prioritised the development of well-formed APIs have been able to overcome interoperability problems, even when the data are not yet in a standardised format.

The development and adoption of (open) APIs for data portability

The issue of standards and interoperability also raises questions on the role and governance of APIs, the software specifications used to facilitate communication and data sharing between information systems. Implementation of these interfaces presents an important digital security challenge (see section above), and also raises questions of the role of IPRs as means to control data access and sharing. There is a lively debate in the United States (and possibly in other countries) as to whether copyright protections attach to APIs and when the fair use defence applies. Other challenges include determining who is responsible financially and who bears legal liability for the ongoing maintenance of APIs. This could include cases where a single developer who developed an API was insufficiently supported despite an accumulation of downstream dependencies.

APIs also reduce the necessity of "data scraping" (or "screen scraping"). At the Online Workshop, participants confirmed the use of APIs was vastly better than "data scraping", which lacks data integrity and was expensive. However, they also noted that APIs would need to be standardised and performance tested to be successful. Participants agreed that APIs, including open source APIs, would make the data transfer process smoother. However, some did not believe a lack of open source APIs was a barrier to portability of data between platforms. Some also questioned the legal status of data scraping, while others suggested that legislation to promote APIs could be combined with legislation to ban data scraping. Others thought data scraping might subvert anti-competitive practices or provide a way to bypass outdated or poorly implemented APIs.

On API governance, differences in requirements may also present challenges as illustrated by PSD2 and the Open Banking regulation in the United Kingdom. PSD2 leaves open implementation details of the APIs needed by third parties to connect with financial services. Meanwhile, the Competition & Markets Authority (CMA) of the United Kingdom requires British banks to set up an independent Open Banking Implementation Entity (OBIE) (OBIE, 2020[85]). OBIE, a non-profit organisation, is funded by nine of the

largest banks and building societies in the United Kingdom (OBIE, n.d.[86]). It is responsible for developing and maintaining the OBIE open banking standards, among others.[37]

To help fill the gap left open by PSD2, the European Banking Authority issued Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 (EBA, 2017[87]). These were complemented by additional frameworks such as the open Finance API Framework (The Berlin Group, 2020[88]) and NextGenMobileP2P (The Berlin Group, 2020[89]). These were developed and maintained by the Berlin Group, "a pan-European payments interoperability standards and harmonisation initiative".[38]

Costs of compliance and the role of trusted third parties

Implementing data portability can involve significant costs to the data holder, as well as to potential data users. These typically include two streams of costs: i) the up-front cost of aggregating data and investments in information technology (IT) systems and networks; and ii) the operational cost for handling data transfer requests and maintaining the systems and networks (Australian Government, Department of Treasury, 2017[79]; Productivity Commission, 2017[8]; Plaitakis and Staschen, 2020[90]). The up-front costs also involve non-IT costs. These include, for instance, the cost of deploying the IT needed to enable data portability, expanding human resources associated with digital tools to transfer data, and other costs related to change management inside the organisations (ODI and Fingleton Associates, 2014[91]). Responses to the Online Platform Survey suggest these costs can increase significantly over time, especially where data portability regulations are changing. This is also challenging for users.

Estimates of the implementation cost of data portability

The implementation costs of data portability can be estimated from survey results about the midata initiative in the United Kingdom and the UK's Open Banking regulations. The Impact Assessment for midata estimates the cost associated with enabling data download by customers (BIS, 2012[92])Most costs are estimated to come from changes in IT systems to convert data on personal transactions or consumption data into relevant data formats. This type of cost is one-off and includes costs for designing a user interface; investment in IT hardware to present information in a secure manner; and installing, commissioning and testing of the facilities system.[39]

The one-off cost tends to be small for a minority of businesses whose data are already in a suitable form. For the majority, the cost of converting data in a suitable format depends on the required change in IT systems. Costs tend to be small when data are acquired and stored for customers who use them for activities such as billing and usage notification. Costs tend to be higher in many retail companies where the data are collected and analysed for providing special offers to customers. Operational costs of providing data portability in contrast are estimated to be generally much smaller but also vary by sector.[40] Overall, small businesses are estimated to incur larger costs to enable data downloading. These costs can be ten times larger per customer for small retail businesses sector compared to other larger businesses, with the exceptions of web-based businesses.[41]

The role of trusted third parties in reducing transaction and compliance costs

Data portability implementation costs may also include technical costs (e.g. for developing or accessing a secure API), transactions and legal costs. These costs and their allocation, in turn, depend on the data transfer scheme. Centralised and decentralised data transfer models, for example, are distinguished by whether a trusted third party is involved and acts as data transfer hub.

In the centralised data transfer model, a trusted third party is used to manage transfer requests from data subjects, and to authenticate and mediate the data transfers. For example, in the United Kingdom, the data subject requests transfer of energy consumption data stored in the second generation of smart meters to

the designated data recipient. This transfer occurs via a communication network centrally managed by Data Communications Company (DCC). DCC authenticates both the data subject requests and the designated data recipients (BEIS, 2018[66]). This model reduces up-front costs for data holders and recipients, as well as the costs of authenticating requests and recipients.

However, centralised models may also incur high costs in building and running the hub, as well as costs associated with data exchanges (ACCC, 2019[93]). In the case of the energy sector in the United Kingdom, for instance, cost recovery of the DCC hub may include charges for energy suppliers, network operators and other authorised users (DCC, n.d.[94]). DDC's total costs are estimated to GBP 626 million in 2021/22 (ending 31 March 2022) (DCC, 2021[95]).

Decentralised models rely on peer-to-peer linkages between data holders and data recipients. Accordingly, the number of potential links are much larger than in centralised models. They also entail up-front and running costs to initiate and maintain data linkages (which may differ from each other in technical specifications and operational rules). Nevertheless, technological and operational standardisation of data transfer is considered to reduce costs (Australian Government, Department of Treasury, 2017[79]; ODI and Fingleton Associates, 2014[91]).

In the context of open banking, co-ordination bodies often assume standardisation roles. The associated costs of such bodies may vary for different open banking initiatives. For instance, in the United Kingdom, the OBIE, as highlighted above, defines API specifications used by banks and data recipients to communicate with each other. In the Australian banking sector, the government runs the co-ordinating body. In addition, Data61 (the data and digital specialist unit of the Australian National Science Agency) was involved in the development and delivery of the federal government's CDR (Data61, n.d.[96]). Data61 was also appointed to perform the role of a data standards body for the CDR.

Cross-agency regulatory co-operation and co-ordination

As highlighted above, data portability initiatives address issues at the intersection of competition, privacy and consumer protection. Therefore, their development and implementation require interdisciplinary co-operation in both policy making and enforcement. Even if only one of these three areas is the primary motivation for a data portability initiative, the process will likely implicate the others. Additionally, other regulatory domains may be implicated when data portability is implemented at a sectoral level (e.g. the Open Banking Initiative), which also involved the financial market authorities.

Respondents of the Online Platform Survey also highlighted the increased need for co-operation and co-ordination across policy areas and regulatory authorities, especially across competition, consumer protection and privacy. They also stressed the need for a comprehensive, internationally recognised framework for data portability.

The Online Expert Consultations also confirmed the importance of cross-agency regulatory co-operation and co-ordination. At the Webinar on Data Portability, experts stressed the need for competition authorities to take data portability rights into account – including those granted by privacy and data protection frameworks such as the EU GDPR – when they assess competition cases. The European Commission (2016[97]) Microsoft/LinkedIn decision was presented as an example. Participants questioned if compliance with privacy and data protection frameworks should be considered more systematically as a condition of approving mergers of data-intensive firms (Graef, Clifford and Valcke, 2018[98]; Graef, 2020[99]).

Enhanced co-operation and co-ordination across agencies has also been discussed in multiple OECD reports (OECD, 2020[100]; OECD, 2020[101]; OECD, 2019[102]; OECD, 2018[103]; OECD, 2019[104]; OECD, 2015[34]). Privacy enforcement authorities have long raised this need for closer dialogue between regulators and experts across policy boundaries. This would help achieve the goal of strengthening competition and consumer protection enforcement, and stimulating the market for privacy-enhancing services (EDPS, 2014[105]; EDPS, 2016[106]). For example, EDPS (2014[105]) already noted that:

> There is currently little dialogue between policy makers and experts in these fields. […] It is essential that synergies in the enforcement of rules controlling anti-competitive practices, mergers, the marketing of so-called "free" on-line services and the legitimacy of data processing are explored. This will help to enforce competition and consumer rules more effectively and also stimulate the market for privacy-enhancing services.

OECD (OECD, 2020[21]) notes the co-ordination of competition and consumer policy issues and enforcement was generally more straightforward in more than 30 jurisdictions where a common agency assumes these responsibilities. This was facilitated thanks to legislative provisions that provide the legal basis for co-operation between these authorities, as is the case, for example, in Germany (Stauber, 2019[107]). Less formal means of co-operating are also available. In 2016, for example, the European Data Protection Supervisor recommended creation of a "Digital Clearinghouse" to facilitate information sharing between regulators relating to possible violations in online markets (EDPS, 2016[106]). It was created through a 2017 Resolution of the European Parliament and brings together regulators across a range of policy areas both from within the European Union and internationally (European Parliament, 2017[108]). In May 2021, the United Kingdom's CMA and ICO issued a joint statement. The statement emphasises "the strong synergies that exist between the aims of competition and data protection, the ways that the two regulators will work collaboratively to overcome any perceived tensions between their objectives, [and] practical examples of how the two organisations are already working together to deliver positive outcomes for consumers" (CMA and ICO, 2021[109]).

At the Webinar on Data Portability, experts discussed the following possible modalities for co-operation between authorities:

- *Mutual consultation*: one authority would seek the views and opinions of another relevant authority. Such consultation would typically be based on a memorandum of understanding or on legislation requiring consultation before decisions are reached.
- *Parallel or joint investigations*: two or more authorities would engage in a joint investigation or undertake their respective investigations independently but co-ordinate their efforts by sharing relevant information to the extent permitted by law.
- *Joint design of remedies and policies:* two or more authorities would collaborate to develop and implement remedies. This could involve dividing up responsibilities so that, for example, competition authorities would impose remedies that Privacy Enforcement Authorities (PEA) would monitor.

When it comes to data portability, collaboration between competition, consumer protection and privacy and data protection enforcement authorities can be challenging. This is largely due to different perceptions among authorities about the purpose of a data portability initiative even though it may strengthen competition, privacy and consumer protection simultaneously. This is in line with views expressed at the Online Expert Discussion, where participants distinguished between viewing data portability through the lens of "privacy and data protection" and the lens of "competition". The desirability of data portability through the competition lens will depend primarily on its effects on choice and innovation. The desirability of data portability through a privacy and data protection perspective might look more at its ability to achieve informational self-determination.

According to Lynskey (2017[13]), for example, data portability in the case of the GDPR forms part of a "bundle of micro rights" designed to give individuals control over their personal data. It sits coherently within a data protection framework, particularly insofar as it remedies (or seeks to remedy) the asymmetry of power between data subject and data controller. In this sense, it is linked to the concept of informational self-determination. In contrast, Australia's CDR is primarily a consumer- and competition-oriented right. It therefore involves three main parties: the consumer (the person or organisation that accesses their data electronically); the data holder (who holds the data about consumer); and the data recipient (the one engaged by the consumer to access the data held by the data holder).

Conclusions and possible areas for further work

Policy discussions on data portability have recently intensified, especially since the adoption of the GDPR, the CCPA and Australia's CDR. There is an increasing interest among countries to implement or at least explore data portability as a means to enhance competition and innovation, and to strengthen the control rights of individuals over their personal data and of businesses (in particular SMEs) over their business data.

Various forms of data portability initiatives and arrangements have thus emerged, including in the private sector. They differ significantly in terms of their scope, legal, technical and organisational requirements. All this has made it difficult to compare data portability initiatives. To some extent, it has created some confusion given the term "data portability" is not always used consistently.

This study aimed, in large part, to contribute to a common understanding of data portability and its economic and social effects. It proposes a working definition and taxonomy through which data portability arrangements and initiatives are differentiated and categorised. In particular, it shows how six key dimensions can be used for an initial mapping of selected well-known and documented data portability initiatives in the private and public sector.

Analysis of the opportunities and challenges of data portability and of its economic and social effects was in part hampered by the scarcity of empirical literature and available quantitative evidence on the economic and social benefits and risks of data portability.

Relatedly, another area that warrants more work is the relationship between data portability and interoperability. While interoperability is generally promoted as data transfer enabler, it is still not regarded as an essential objective of most data portability regimes. The relationship between interoperability, competition and innovation seems to depend on context. Nonetheless, governments and regulators in certain jurisdictions and sectors are increasingly exploring data portability regimes that enable real-time continuous data transfers and the interoperability of digital services, in particular at the sectoral level (data portability 3.0). This is to some extent also true in the European Union where there are calls for measures to complement Art. 20 of the GDPR (on the right to data portability) with additional interoperability requirements such as, to some extent, via the new EU Data Governance Act.

The report also points to an increasing need for cross-agency regulatory co-operation and co-ordination, especially in areas where data portability is cross-sectoral. In most cases, data portability involves personal data and can be motivated by privacy, consumer and competition enforcement considerations. This requires multidisciplinary enforcement collaboration, particularly when other sector-specific regulators are concerned.

Finally, the report highlights the important role of trusted third-party intermediaries for data portability and interoperability. It argues that data portability could stimulate creation of new business models, including data intermediaries that promise to restore user agency. Examples include PIMS, PDS and the Information Trust Bank. These intermediaries may help reduce transaction and compliance costs. However, the centralisation of data transfer schemes that comes with an increased role of these intermediaries can generate risks, including to competition, privacy and consumer protection. The analysis of these risks and of the criteria needed by these intermediaries to be considered "trusted" was outside the scope of this report. It deserves to be addressed in dedicated future work.

References

ACCC (2020), *Digital Advertising Services Inquiry Interim Report*, Australian Competition and Consumer Commission, Canberra, https://www.accc.gov.au/system/files/Digital%20Advertising%20Services%20Inquiry%20-%20Interim%20report.pdf. [18]

ACCC (2019), "Consumer data right in energy", *Position Paper: Data Access Model for Energy Data*, Australian Competition and Consumer Commission, Canberra, https://www.accc.gov.au/system/files/ACCC%20-%20CDR%20-%20energy%20-%20data%20access%20models%20position%20paper%20-%20August%202019.pdf. [93]

Apple (n.d.), "Transfer a Copy of Your iCloud Photos Collection to Another Service", webpage, https://support.apple.com/en-us/HT208514 (accessed on xxx xx 2021). [115]

Article 29 Data Protection Working Party (2017), *Guidelines on the Right to Data Portability*, Article 29 Data Protection Working Party, Brussels, https://ec.europa.eu/newsroom/just/redirection/document/44099. [84]

Australian Competition and Consumer Commission (2020), *Energy rules frameworkConsultationpaper*, https://www.accc.gov.au/system/files/CDR%20-%20Energy%20rules%20framework%20consultation%20paper%20-%20July%202020_0.pdf (accessed on 10 February 2021). [127]

Australian Government, Department of Treasury (2017), *Open Banking: Customers, Choice, Convenience, Confidence*, Department of the Treasury, Government of Australia, https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf. [79]

Auxier, B. et al. (2019), "Americans and privacy: Concerned, confused and feeling lack of control over their personal information", 15 November, Pew Research Center, Washington, DC, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. [77]

Axway (2020), *Open Banking APIs State of the Market Report 2020*, Axway, Phoenix, Arizona, https://resources.axway.com/financial-services/report-open-banking-in-an-age-of-transformation. [61]

BEIS (2018), *Implementing Midata in the Energy Sector: Call for Evidence*, Department for Business, Energy & Industrial Strategy, Government of the United Kingdom, http://dx.doi.org/www.gov.uk/government/consultations/call-for-evidence-implementing-midata-in-the-energy-sector. [58]

BEIS (2018), *Smart Metering Implementation Programme: Review of the Data Access and Privacy Framework*, Department for Business, Energy & Industrial Strategy, Government of United Kingdom, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758281/Smart_Metering_Implementation_Programme_Review_of_the_Data_Access_and_Privacy_Framework.pdf. [66]

BIS (2012), *midata: Government response to 2012 consultation*, Department for Business Innovation & Skills, Government of the United Kingdom, http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34700/12-1283-midata-government-response-to-2012-consultation.pdf. [111]

BIS (2012), *midata: Impact Assessment for midata*, Department for Business Innovation & Skills, Government of the United Kingdom, http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32689/12-944-midata-impact-assessment.pdf. [92]

BIS (2011), *Better Choices: Better Deals – Consumers Powering Growth*, Department for Business Innovation & Skills, Government of the United Kingdom. [110]

Black, K. (2021), "Cheers to heightened health (privacy) in 2021", *National Law Review*, Vol. 19 January, https://www.natlawreview.com/article/cheers-to-heightened-health-privacy-2021. [7]

Brown, I. and D. Korff (1 October 2020), "Interoperability as a tool for competition regulation", Tech Blog, https://www.ianbrown.tech/2020/10/01/interoperability-as-a-tool-for-competition-regulation-2/. [45]

Business, Energy, and Industrial Strategy (2018), *Smart Metering Implementation Programme: review of the Data Access and Privacy Framework*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758281/Smart_Metering_Implementation_Programme_Review_of_the_Data_Access_and_Privacy_Framework.pdf (accessed on 10 February 2021). [126]

Catapult Energy System (2018), "An Introduction to Interoperability in the Energy Sector", (brochure), Catapult Energy System, Birmingham, UK, https://es.catapult.org.uk/brochures/an-introduction-to-interoperability-in-the-energy-sector/#. [41]

Center for Medicare and Medicaid Services (2018), *Blue Button 2.0 Implementation Guide*, website, https://bluebutton.cms.gov/assets/ig/index.html (accessed on 1 March 2021). [123]

Chen, J. (2016), "How do switching costs affect market concentration and prices in network industries?", *Journal of Industrial Economics*, Vol. 64/2, pp. 226-254, https://onlinelibrary.wiley.com/doi/full/10.1111/joie.12102. [52]

Choy, N. (2020), "Open banking APIs a bigger threat to Singapore banks than digital entrants: DBS Research", 25 February, The Business Times, https://www.businesstimes.com.sg/banking-finance/open-banking-apis-a-bigger-threat-to-singapore-banks-than-digital-entrants-dbs. [48]

CMA (2020), *J1 Appendix J: Facebook Platform and API Access*, Competition and Markets Authority, London, https://assets.publishing.service.gov.uk/media/5efb1dd2d3bf7f7699160dd6/Appendix_J_-_Facebook_Platform_and_API_access_v4.pdf. [46]

CMA (2020), *Online Platforms and Digital Advertising Market Study*, Competition & Markets Authority, London, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study. [17]

CMA and ICO (2021), *Competition and Data Protection in Digital Markets: A Joint Statement between the CMA and the ICO*, Competition & Markets Authority, Information Commissioner's Office, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf. [109]

Ctrl-Shift (2018), "Data mobility: The personal data portability growth opportunity for the UK economy", report commissioned by Department for Digital, Culture, Media and Sport, Ctrl-Shift, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755219/Data_Mobility_report.pdf. [70]

Data61 (n.d.), "Consumer Data Standards", webpage, https://data61.csiro.au/en/Our-Research/Focus-Areas/Special-Projects/Consumer-Data-Standards (accessed on xx xx 2021). [96]

DCC (2021), *Indicative Budget Regulatory Years ending 31 March 2023 and 2024*. [95]

DCC (n.d.), "Charging Methodology, Statements & Budgets", webpage, https://www.smartdcc.co.uk/document-centre/charging-methodology-statements-budgets/ (accessed on 10 February 2021). [94]

De Hert, P. et al. (2018), "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer Law and Security Review*, Vol. 34/2, pp. 193-203, http://dx.doi.org/10.1016/j.clsr.2017.10.003. [55]

de la Mano, M. and J. Padilla (2018), "Big tech banking", *Journal of Competition Law & Economics*, Vol. 14/4, pp. 494-526, https://doi.org/10.1093/joclec/nhz003. [27]

Di Porto, F. and G. Ghidini (2020), ""Access Your Data, You Access Mine" – Requiring Data Reciprocity in Payment Services", *International Review of Intellectual Property and Competition Law*, Vol. 307/51. [28]

DTP (n.d.), *Data Transfer Project*, website, https://datatransferproject.dev/ (accessed on 1 March 2021). [118]

EBA (2017), "Regulatory technical standards on strong customer authentication and secure communication under PSD2", *Final Report*, European Banking Authority, Paris, http://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf. [87]

EDPS (2016), *EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data*, Opinion 8/26, European Data Protection Supervisor, Brussels, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf. [106]

EDPS (2014), "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", 26 March, Preliminary Opinion, European Data Protection Supervisor, Brussels, https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en. [105]

Egan, E. (2020), *Data Portability and Privacy*, Facebook, https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf. [82]

Engels, B. (2016), "Data portability among online platforms", *Internet Policy Review*, Vol. 5/2, https://doi.org/10.14763/2016.2.408. [73]

EU (2019), *Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information*, EUR-Lex, http://data.europa.eu/eli/dir/2019/1024/oj. [139]

EU (2013), *Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information*, EUR-Lex, http://data.europa.eu/eli/dir/2013/37/oj. [140]

European Commission (2021), "Free Flow of Non-personal Data", webpage, https://digital-strategy.ec.europa.eu/en/policies/non-personal-data (accessed on 23 June 2021). [30]

European Commission (2021), "Presentation of Codes of Conduct on cloud switching and data portability", 9 December, News, European Commission, Brussels, https://digital-strategy.ec.europa.eu/en/news/presentation-codes-conduct-cloud-switching-and-data-portability. [33]

European Commission (2016), *Regulation (EC) No 139/2004 Merger Procedure*, European Commission, Brussels, https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf. [97]

European Parliament (2017), *Report on Fundamental Rights Implications of Big Data: Privacy, Data protection, Non-discrimination, Security and Law enforcement*, European Parliament, Brussels, https://www.europarl.europa.eu/doceo/document/A-8-2017-0044_EN.pdf. [108]

European Union (2018), *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*, European Union, Brussels, http://data.europa.eu/eli/reg/2018/1807/oj. [29]

European Union (2016), "Recital 68 of GDPR", webpage, https://gdpr-info.eu/recitals/no-68/ (accessed on xxx xx 2021). [54]

European Union (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, European Union, Brussels, http://data.europa.eu/eli/reg/2016/679/oj. [2]

Eurostat (2019), "Security related problems experienced through using the internet for private purposes (isoc_cisci_pb)", *Digital Economy and Society*, (database), http://www.urlfordatabase (accessed on 28 January 2020). [42]

FCA (2015), *Making Current Account Switching Easier*, Financial Conduct Authority, London, https://www.fca.org.uk/publication/research/making-current-account-switching-easier.pdf. [50]

FTC (2015), "Start with Security: A Guide For Business", webpage, http://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (accessed on 21 June 2021). [80]

FTC (2014), "FTC puts conditions on CoreLogic, Inc.'s proposed acquisition of DataQuick Information Systems", 24 March, Press Release, Federal Trade Commission, Washington, DC, http://www.ftc.gov/news-events/press-releases/2014/03/ftc-puts-conditions-corelogic-incs-proposed-acquisition-dataquick. [20]

Gallaher, M. (2020), "Trade agreements to move the digital economy", December, Visa Economic Empowerment Institute, https://usa.visa.com/sites/visa-economic-empowerment-institute/growth-through-trade/trade-agreements-to-move-digital-economy.html. [142]

Gal, M. and D. Rubinfeld (2019), "Data standardization", *New York University Law Review*, Vol. 94/4, pp. 737-770, https://www.nyulawreview.org/issues/volume-94-number-4/data-standardization/. [44]

Github (n.d.), *google/data-transfer-project*, website, https://github.com/google/data-transfer-project (accessed on 1 March 2021). [119]

Goverment of the United Kingdom (2013), *Enterprise and Regulatory Reform Act 2013*, legislation.goverment.uk, http://www.legislation.gov.uk/ukpga/2013/24/contents. [112]

Graef, I. (2020), "The opportunities and limits of data portability for stimulating competition and innovation", *Competition Policy International Antitrust Chronicle*, pp. 1-8, https://ssrn.com/abstract=3740185. [99]

Graef, I., D. Clifford and P. Valcke (2018), "Fairness and enforcement: Bridging competition, data protection and consumer law", *International Data Privacy Law 2018*, Vol. 8/3, pp. 200-223, https://ssrn.com/abstract=3216198. [98]

Graef, I., M. Husovec and N. Purtova (2018), "Data portability and data control: Lessons for an emerging concept in EU law", *German Law Journal*, Vol. 19/6, pp. 1359-1398, http://dx.doi.org/10.1017/S2071832200023075. [15]

Graef, I., S. Wahyuningtyas and P. Valcke (2015), "Assessing data access issues in online platforms", *Telecommunications Policy*, Vol. 39/5, pp. 375-387, https://doi.org/10.1016/j.telpol.2014.12.001. [72]

Graham-Jones, P. and R. Panchadsaram (5 February 2013), "Introducing Blue Button+", Health IT Buzz, Consumer Engagement Blog, http://www.healthit.gov/buzz-blog/consumer/introducing-blue-button. [122]

Gross, C. (4 May 2021), "CPRA vs. CCPA: What's the difference? 6 key changes to understand", A-Lign Blog, https://a-lign.com/cpra-vs-ccpa/ (accessed on 28 June 2021). [117]

HDMC (2020), *Interim Report on the Evaluation of Competition in the Digital Advertising Market Summary*, Headquarters for Digital Market Competition of the Japanese Cabinet Office, Tokyo, https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_200616-1.pdf. [23]

HDMC (2020), *Report on Medium-Term Vision on Competition in the Digital Market: Summary*, Headquarters for Digital Market Competition of the Japanese Cabinet Office, Tokyo, https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_200616-2.pdf. [19]

HSS (2020), "HHS proposes modifications to the HIPAA privacy rule to empower patients, improve coordinated care, and reduce regulatory burdens", (fact sheet), 10 December, Department of Health and Human Services, Office for Civil Rights, Washington, DC, http://www.hhs.gov/about/news/2020/12/10/hhs-proposes-modifications-hipaa-privacy-rule-empower-patients-improve-coordinated-care-reduce-regulatory-burdens.html. [5]

HSS (2020), *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement*, 45 CFR Parts 160 and 164, Department of Health and Human Services, Office for Civil Rights, Washington, DC, http://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf. [6]

IAPP (2021), "The California Privacy Rights Act of 2020", webpage, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/ (accessed on 21 June 2021). [116]

IIF (2018), "Liability and consumer protection in open banking", September, Institute of International Finance, Washington, DC, https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf. [83]

Information Commissioner's Office (UK) (2020), *Encryption*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/. [134]

IRENA (2020), *Innovation Landscape Brief: Energy as a Service*, International Renewable Energy Agency, Abu Dhabi, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2020/Jul/IRENA_Energy-as-a-Service_2020.pdf?la=en&hash=E81F973296F812182DB6E44804695344CEADE848. [65]

ISO (2017), "ISO/IEC 19941:2017(en) Information technology – Cloud computing – Interoperability and portability", webpage, https://www.iso.org/obp/ui/#iso:std:iso-iec:19941:ed-1:v1:en (accessed on 9 March 2021). [39]

Janal, R. (2017), "Data portability – A tale of two concepts", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 8/1, pp. 59-69. [14]

JFTC, METI, MIC (2019), "Options for rulemaking to address the rise of platform businesses", 21 May, Joint Press Release, Ministry of Economy Trade and Industry, Japan Fair Trade Commission, Ministry of Internal Affairs and Communications, Tokyo, https://www.meti.go.jp/english/press/2019/0521_006.html. [22]

JFTC, METI, MIC (2019), *Options for Rulemaking to Address the Rise of Platform Businesses Released*, https://www.meti.go.jp/english/press/2019/0521_006.html. [128]

Kerber, W. (2021), "From (horizontal and sectoral) data access solutions towards data governance systems", *Joint Discussion Paper Series in Economics*, No. 40-2020, Universities of Aachen · Gießen · Göttingen Kassel · Marburg · Siegen. [26]

Kerber, W. (2019), "Data sharing in IoT ecosystems and competition law: The example of connected cars", *Journal of Competition Law & Economics*, Vol. 15/4, pp. 381-426, http://dx.doi.org/10.1093/joclec/nhz018. [57]

Krämer, J., P. Senellart and A. Streel (2020), *Making Data Portability More Effective for the Digital Economy*, CERRE, Brussels, https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/. [25]

LifeSREDA (2016), *Overview of APIs and Bank-as-a-Service in FINTECH*, LifeSREDA, Singapore, https://www.bank-as-a-service.com/BaaS.pdf. [60]

Lynskey, O. (2017), "Aligning data protection rights with competition law remedies? The GDPR right to data portability", *European Law Review*, Vol. 42. [13]

MacCarthy, M. (2020), "Should policymakers slay the tech titans or force them to behave?", 10 June, Apolitical, https://apolitical.co/en/solution_article/should-policymakers-slay-the-tech-titans-or-force-them-to-behave. [71]

Mathur, A., M. Boyd and P. Pham (1 June 2020), "Q3 2020 Open Banking API Trends Datapoint: Global platforms", Open Banking/Open Finance Blog, https://platformable.com/q3-open-banking-api-trends-datapoint-global-platforms. [62]

Microsoft et al. (2019), *Data Transfer Project*, https://datatransferproject.dev/. [120]

MyData Global (n.d.), "About", webage, https://mydata.org/about/organisation/ (accessed on 12 March 2021). [121]

Nicholas, G. (2020), "Taking it with you: Platform barriers to entry and the limits of data portability", *Michigan Telecommunications and Technology Law Review*, Vol. Forthcoming, p. 31, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3550870. [43]

Nissenbaum, H. (2004), "Privacy as contextual integrity", *Washington Law Review*, Vol. 79/1, pp. 119-157, https://nyuscholars.nyu.edu/en/publications/privacy-as-contextual-integrity (accessed on 24 March 2018). [143]

OAIC (2021), "CDR Privacy Safeguard Guidelines", webpage, http://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/ (accessed on xx xx 2021). [37]

OAIC (2017), *Australian Community Attitudes to Privacy Survey 2017*, Office of the Australian Information Commissioner, Sydney, https://www.oaic.gov.au/updates/videos/australian-community-attitudes-to-privacy-survey-2017/. [78]

OAIC (n.d.), "CDR participants", webpage, http://www.oaic.gov.au/consumer-data-right/cdr-participants/ (accessed on 29 June 2021). [38]

OBIE (2020), *Annual Report 2020*, Open Banking, London, https://assets.foleon.com/eu-west-2/uploads-7e3kk3/48197/obie-ra-artwork-10096a5716bf30-2.5853a6c2c203.pdf. [85]

OBIE (n.d.), "Open Banking", webpage, https://www.openbanking.org.uk/about-us/ (accessed on 10 February 2021). [86]

ODI and Fingleton Associates (2014), *Data Sharing and Open Data for Banks: A Report for HM Treasury and Cabinet Office*, Open Data Institute and Fingleton Associates, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF. [91]

OECD (2021), "Data portability, interoperability and digital platform competition", *OECD Competition Committee Discussion Paper*, http://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf. [16]

OECD (2021), "Digital Trade Inventory", No. TAD/TC/WP(2020)14/FINAL, Trade and Agriculture Directorate, OECD, Paris, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)14/FINAL&docLanguage=En. [138]

OECD (2020), "Consumer data and competition: A new balancing act for online markets?", *Going Digital Tookit Policy Note*. [129]

OECD (2020), "Consumer data and competition: A new balancing act for online markets?", *Going Digital Toolkit Policy Note*, No. DAF/COMP(2020)18/FINAL, Directorate for Financial and Enterprise Affairs, Competition Committee, OECD, Paris, https://one.oecd.org/document/DAF/COMP(2020)18/FINAL/en/pdf. [21]

OECD (2020), "Consumer Data Rights and Competition", webpage, https://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm (accessed on xx xx 2021). [100]

OECD (2020), *Enhanced Access to Publicly Funded Data for Science, Technology and Innovation*, OECD Publishing, Paris, https://dx.doi.org/10.1787/947717bc-en. [11]

OECD (2020), "Going Digital integrated policy framework", *OECD Digital Economy Papers*, No. 292, OECD Publishing, Paris, https://dx.doi.org/10.1787/dc930adc-en. [101]

OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, https://dx.doi.org/10.1787/53e5f593-en. [1]

OECD (2019), "Challenges to consumer policy in the digital age", *Background Report G20 International Conference on Consumer Policy*, OECD, Paris, https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf. [104]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://dx.doi.org/10.1787/276aaca8-en. [9]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://dx.doi.org/10.1787/276aaca8-en. [35]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://dx.doi.org/10.1787/276aaca8-en. [146]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264312012-en. [102]

OECD (2019), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/059814a7-en. [12]

OECD (2019), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/059814a7-en. [145]

OECD (2018), *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264305847-en. [10]

OECD (2018), *Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers*, Directorate for Science, Technology and Innovation, OECD, Paris, https://www.oecd.org/going-digital/topics/digital-consumers/toolkit-for-protecting-digital-consumers.pdf. [103]

OECD (2017), *Digital risk and trust*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264276284-9-en. [81]

OECD (2016), "Research Ethics and New Forms of Data for Social and Economic Research", *OECD Science, Technology and Industry Policy Papers*, No. 34, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jln7vnpxs32-en. [49]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264229358-en. [125]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [130]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [131]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [132]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [133]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [135]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [34]

OECD (2014), *Summary of OECD Expert Roundtable Discussion on "Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking"*, Directorate for Science, Technology and Industry, OECD, Paris, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en. [36]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, amended on 11 July 2013 - C(2013)79, http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=114. [4]

OECD (2013), *The OECD Privacy Framework*, OECD, Paris, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [3]

OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 176, OECD Publishing, Paris, https://dx.doi.org/10.1787/5kgf09z90c31-en. [76]

Ofgem (2010), *Smart Metering Implementation Programme: Statement of Design Requirements*, Office of Gas and Electricity Markets, Government of United Kingdom, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/42723/225-smart-metering-imp-programme-design.pdf. [40]

Open Banking Expo (2018), *How Open Banking became a catalyst for mergers*, http://www.openbankingexpo.com/news/how-open-banking-became-a-catalyst-for-mergers/. [137]

Open Banking Limited (n.d.), "Meet the Regulated Providers", webpage, https://www.openbanking.org.uk/customers/regulated-providers/ (accessed on xx xx 2021). [51]

Pham, P., M. Boyd and A. Mathur (13 August 2020), "Open Banking Trends Q2 2020: Banks", Open Banking/Open Finance Blog, https://platformable.com/blog/q2-open-banking-trends-banks/. [63]

Plaitakis, A. and S. Staschen (2020), "Open banking: How to design for financial inclusion", *Working Paper*, Consultative Group to Assist the Poor, Washington, DC, https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Open_Banking.pdf. [90]

Plant, M. (13 January 2021), "Does your health app protect your sensitive info?", Consumer Information Blog, http://www.consumer.ftc.gov/blog/2021/01/does-your-health-app-protect-your-sensitive-info. [141]

Platformable (2020), *Open Banking Quarterly Trends Report 2020*, Platformable, https://trends.platformable.com/open-banking. [64]

Productivity Commission (2017), "Data availability and use", *Productivity Commission Inquiry Report*, No. 82, Productivity Commission, Canberra, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf. [8]

Productivity Commission (2017), *Productivity Commission Inquiry Report: Data Availability and Use*, Productivity Commission, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf. [144]

Rosschke, G. and A. Zach (2020), "Data to go: The FTC's workshop on data portability", November, CPI Antitrust Chronicle, https://www.ftc.gov/system/files/documents/public_events/1568699/data-portability-workshop-summary.pdf. [56]

Ruth, J. (2017), "Data Portability – A Tale of Two Concepts", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 58/62. [74]

Services, D. (2020), *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement*, https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf. [136]

Solid (n.d.), "About Solid", webpage, https://solidproject.org/about (accessed on xx xx 2021). [124]

Specht-Riemenschneider, L. (2021), "Data access rights – A comparative perspective", in *Data Access as a Means to Promote Consumer Interests and Public*, http://dx.doi.org/10.5771/9783748924999-401. [24]

Stauber, P. (2019), *Facebook's abuse investigation in Germany and some thoughts on cooperation between antitrust and data protection authorities*, February, CPI Antitrust Chronicle, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf. [107]

Suleymanova, I. and C. Wey (2011), "Bertrand competition in markets with network effects and switching costs", *The B.E. Journal of Economic Analysis & Policy*, Vol. 11/1, https://doi.org/10.2202/1935-1682.2359. [53]

SWIPO (2020), *Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service*, 27 May, The Association on Switching and Porting, Brussels, https://swipo.eu/wp-content/uploads/2020/10/SWIPO-IaaS-Code-of-Conduct-version-2020-27-May-2020-v3.0.pdf. [31]

SWIPO (2020), *Switching and Portability of Data related to Software as a Service (SaaS)*, The Association on Switching and Porting, Brussels, https://swipo.eu/wp-content/uploads/2020/07/SWIPO-SaaS-Code-of-Conduct.pdf. [32]

Swire, P. and Y. Lagos (2013), "Why the right to data portability likely reduces consumer welfare: Antitrust and privacy critique", *Ohio State Public Law Working Paper*, No. 204, Ohio State University, http://dx.doi.org/10.2139/ssrn.2159157. [67]

The Berlin Group (2020), "Berlin Group starts new openFinance API Framework", 16 October, Press Release, Berlin Group, Bonn, http://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework. [88]

The Berlin Group (2020), "NextGenMobileP2P Downloads", webpage, http://www.berlin-group.org/nextgenmp2p-download-page (accessed on xx xx 2021). [89]

Trustpilot (2018), "Open Banking expected to contribute over £1 billion annually to UK economy supporting 17,000 new jobs", 26 February, Company Announcement, Trustpilot, Copenhagen, http://press.trustpilot.com/news/2018/2/26/open-banking-expected-to-contribute-over-1-billion-annually-to-uk-economy-supporting-17000-new-jobs. [69]

Tsotsis, A. (2010), "Facebook now allows you to 'download your information'", 6 October, TechCrunch, https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/. [114]

United Kingdom ICO (2019), *Right to data portability*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (accessed on 20 January 2020). [75]

Urquhart, L., N. Sailaja and D. Mcauley (2017), "Realising the right to data portability for the domestic Internet of things", *Personal and Ubiquitous Computing*, Vol. 22, pp. 317-332, https://doi.org/10.1007/s00779-017-1069-2. [59]

US House Judiciary Committee (2020), *Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations*, US House Judiciary Committee, Washington, DC. [47]

White & Case (2018), "Financial institutions M&A trends: Banks", 28 June, Insight, White & Case, http://www.whitecase.com/publications/insight/financial-institutions-ma-trends-banks-0. [68]

Willard, B. (20 July 2018), "Introducing Data Transfer Project: An open source platform promoting universal data portability", Google Open Source Blog, https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html. [113]

Annex A: Mapping data portability initiatives in the private and public sector

Data portability has been the focus of a number of different policy initiatives since at least 2010. However, these initiatives differ considerably in terms of their purpose, scope (e.g. who has the right to have data ported and what data can be ported), exceptions to mandatory porting and consequences for non-compliance.

This section provides an initial mapping of selected well-known and documented government and private sector initiatives. It draws on the *modus operandi* to structure and present a number of data portability initiatives that reflects historical developments. It begins with early initiatives, referred to as "data portability 1.0" in this report, that introduced the ad hoc download of data in commonly used machine-readable structured formats (e.g. the 2010 "My Data" initiatives in the United States). It continues to ad hoc direct transfers of data to another data holder ("data portability 2.0" as promoted by the GDPR, for example. It then moves to sector-specific data portability (3.0) initiatives that in some cases mandate implementation of open APIs (e.g. Open Banking Initiative in the United Kingdom). The five key dimensions of each initiative are briefly highlighted.

Data portability 1.0: Ad hoc data downloads

The midata initiative of the United Kingdom

In 2011, the United Kingdom introduced its "midata" Data Portability Initiative (then "mydata") as part of a broader consumer empowerment strategy (BIS, 2011[110]). When launched, the government claimed it was "the first time globally there has been such a Government-backed initiative to empower individuals with so much control over the use of their own data" (OECD, 2015[34]). The programme was initially rolled out in anticipation that release of transaction data would stimulate innovation and the expansion of third-party choice engines such as price comparison websites (BIS, 2012[92]).

- *Beneficiaries and data types*: midata seeks to give consumers access to the electronic information that companies hold about their transactions in a machine-readable and portable format. This "transaction data" includes, for instance, information collected about an individual's browsing history and purchases when logged in to a particular website (BIS, 2012[111]). However, purchases made with a "guest" account entailing no user registration, or information about complaints or other such communications with service providers, would not constitute individual transaction data.
- *Addressees and sectoral scope*: The midata initiative focuses on businesses in three sectors: energy supply; the mobile phone sector; and the financial sector (current accounts and credit cards).

- *Legal obligations*: Rather than legislating to introduce this data portability obligation, the government preferred to "take a power" pursuant to the Enterprise and Regulatory Reform Act 2013 (Goverment of the United Kingdom, 2013[112]). This allows the Secretary of State to introduce regulations to make midata compulsory if the government is unsatisfied with progress in these sectors on a voluntary basis.[42]

- *Modus operandi*: The midata initiative essentially allows consumers to download their current account transactions in a standardised format for easy comparison against accounts offered by other providers. Since then, the United Kingdom government has taken steps to implement midata in the energy sector (BEIS, 2018[58]). The United Kingdom has now adopted legislation mirroring the GDPR, including the right to data portability, and issued guidance to this end.

Private sector initiatives

The private sector, including online platforms, has been investing and innovating in the area of data portability. Since 2007, through its "Google Data Liberation Front" engineering team, Google has been developing data portability tools that allow its users to export a copy of their data from individual Google products. In 2011, with the launch of "Google Takeout", Google provides a single place for users to download a copy of their data and/or to send a copy of their data directly to another service (see next section on data portability 2.0 on the DTP) (Willard, 20 July 2018[113]). In 2010, as another example, Facebook began allowing its users to download their personal data (including profile information, photos, videos, wall posts, event information and a list of friends) (Tsotsis, 2010[114]). Recently, Apple announced that customers in certain jurisdictions can request to transfer a copy of their photos to other services, including Google Photos (Apple, n.d.[115]).

Data portability 2.0: Ad hoc direct transfers of data to another data holder

Health Insurance Portability and Accountability Act (HIPAA) in the United States

HIPAA was introduced in the United States in 1996 to improve the flow and transfer of information related to health care. Among its major goals, HIPAA aimed to make it easier for patients to receive continuity in care if their health insurance coverage changed, such as when changing employer. In 2013, the HITECH Act significantly amended HIPAA to allow for better privacy protection in relation to electronic health records. More recently, the Department of Health and Human Services has proposed changes to the HIPAA privacy rule (which restricts the use and transfer of protected health information) to enable individuals to directly share their patient health information among covered entities (HSS, 2020[6]). This includes requiring electronic patient health information to be provided to individuals at no cost (HSS, 2020[5]; HSS, 2020[6]). These changes are under consultation, but, if adopted, will enhance patients' data portability options.

- *Type of data*: The proposed amendments would allow for easier transfer for protected health information (PHI), being "individually identifiable health information maintained or transmitted by or on behalf of HIPAA covered entities (i.e. health care providers who conduct covered health care transactions electronically, health plans and health care clearinghouses)" (HSS, 2020[6]).

- *Beneficiary*: Currently, under HIPAA, patients can access and obtain a copy of their PHI and provide it to third parties. The proposed rules contemplate individuals' access right to direct copies of their electronic PHI to third parties. This right would require entities covered by HIPAA, including health care providers and health plans, "to submit an individual's access request to another health care provider and to receive back the requested electronic copies of the individual's PHI" in electronic format, thereby avoiding the need for the individual to be involved in the data porting.

- *Addressees and sectoral scope:* HIPAA is a sectoral regulation, as it only applies to certain health information and certain parties involved in providing health care and related services and thus covered by HIPAA.

- *Mandatory or voluntary*: The changes would create a mandatory data porting regime, where covered entities would be required to transfer data upon request by an individual.

- *Modus operandi*: The proposed rules contemplate one-off data transfers between covered entities upon the user's request. While users are also able to request access and receive and deal with data themselves, the proposed regime allows for the user to provide the request to one entity and request the data be provided directly to another entity. The proposed rules would reduce the time in which covered entities are required to respond to an access request from 30 calendar days to 15 calendar days, with the opportunity of a further 15-day extension. The proposed rules also provide for circumstances in which the electronic PHI must be provided at no charge to the individual but allow for fees to be charged for direct transfer to another covered entity.

The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)

The 2018 CCPA, which took effect on 1 January 2020 and started to be enforced from 1 July 2020, incorporates a quasi-data portability obligation. In November 2020, Californians voted to approve the CPRA of 2020, and it will come into effect on 1 January 2023. It will complement the CCPA by updating and extending certain rules and stipulations to enhance the privacy rights of Californian consumers or households, including their rights to data portability.

- *Addressees and sectoral scope*: Pursuant to California Civil Code Section 1798.145(a)(6) and Section 1798.140(c)(1), all companies doing business in California have to comply with the CCPA. An exemption only applies if a company has an annual revenue of less than USD 25 million, collects data from fewer than 50 000 Californians annually and earns less than 50% of its income from its data commerce (Specht-Riemenschneider, 2021[24]). The CPRA has a slightly narrower scope: only those companies with annual buys, sells or shares of the personal information of 100 000 or more Californian consumers or households fall under the scope of the CPRA. Nevertheless, the CPRA has a more extended scope: it includes companies with annual revenues derived from *sharing* personal data in addition to *selling* it (IAPP, 2021[116]; Gross, 4 May 2021[117]).

- *Beneficiaries*: California Civil Code Section 1798.100 provides that a consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

- *Type of data*: Until 1 January 2021, certain data, such as employee data and business communication data, were exempted from the scope of the CCPA (see Assembly Bills 25 and 1355). Assembly Bill 874 clarifies that "personal information" includes information that reasonably identifies, relates to, describes or can reasonably be associated with a particular consumer or household, or could reasonably be associated, directly or indirectly, with a particular consumer or household. The CPRA introduces a new category of protected data: sensitive personal information (SPI), which can be compared to Article 9 of the EU GDPR. Relevant to data portability, and in particular to the transfer of data, is that the "CPRA imposes specific requirements and restrictions on SPI, giving users expanded rights to control businesses' use of their personal information" (Gross, 4 May 2021[117]).

- *Modus operandi*: Businesses that receive a verifiable consumer request from a consumer must "promptly take steps to disclose and deliver, free of charge to the consumer, the customer's

personal information… by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance" (California Civil Code Section 1798.100[d]). However, "a business may provide personal information to a consumer at any time but shall not be required to provide personal information to a consumer more than twice in a 12-month period." While the subject's transmission of the data to another controller was initially contemplated, there is no obligation under the CCPA for controller-to-controller data transfers. This is a major difference to the CPRA: "Now, under the CPRA, a consumer can request that a business transfer specific personal information to another entity 'to the extent technically feasible, in a structured, commonly used, machine-readable format'" (Gross, 4 May 2021[117]). This effectively makes the CPRA a data portability 2.0 initiative.

The "Right to Data Portability" (Art. 20) of the GDPR

The entry into force of the GDPR in May 2018 formalised the right of data portability within the European Union. Whereas the directive that preceded the GDPR gave data subjects the right to access their data,[43] the GDPR went a step further and granted data subjects a separate, distinct right of personal data portability. That right, in Article 20 of the GDPR, provides that the data subject "shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance…". The right applies where processing is based on consent or another legitimate category (Art 9[2]), is necessary for the performance of a contract, or when the processing is carried out by automated means (Art. 20[1]). Recital 68 explains that data controllers "be encouraged to develop interoperable formats that enable data portability" but that the right does not oblige controllers to adopt or maintain processing systems that are technically compatible.

- *Type of data*: The GDPR right only applies to personal data *provided by* the data subject with consent or under contract that is electronically processed. The (former) Article 29 Working Party indicates in accompanying guidance that the definition of personal data should encapsulate data volunteered by the individual or *observed* by virtue of their use of the service or device – but not personal data that is inferred or derived (OECD, 2015[34]).

- *Beneficiary*: For the purposes of the GDPR, "Data subject" only includes natural persons – corporations cannot take advantage of the right to data portability [Art. 4(1)]. The GDPR also provides that the right to data portability also includes "the right to have the personal data transmitted directly from one controller to another, where technically feasible."

- *Addressees and sectoral scope*: The right in the GDPR is "horizontal", in that it applies beyond specific sectors.

- *Mandatory or voluntary*: The GDPR provides a right to data portability; entities subject to the GDPR are obliged to respect it.

- *Modus operandi:* The GDPR provides that the data controller provides "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request". This one month period can be extended to a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request" derived (OECD, 2015[34]).

The regulation for the free flow of data of the European Union

Some months after the GDPR entered into force, the European Union introduced a regulation on a framework for the free flow of *non*-personal data in the European Union.[44] The regulation provides that the European Commission shall encourage the development of Union-level codes of conduct regarding "best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data" (Art. 6[1][a]). The Commission published practical guidance on the regulation in May 2019 with a particular focus on datasets comprised of personal and non-personal data.[45]

- *Type of data*: The regulation for the free flow of data specifically relates to non-personal data. Together, these regulations create a comprehensive framework for the free movement of all types of data (personal and non-personal) within the European Union.

- *Beneficiary*: The FFDRs contemplate data transfers between data holders to enable switching of service providers and the porting of data.

- *Addressees and sectoral scope*: Similar to the GDPR, the FFDR applies generally across all sectors.

- *Mandatory or voluntary:* The FFDR proposes a framework of self-regulation to be developed by businesses. It requires business to develop and implement "self-regulatory codes of conduct" to enable porting to data (Art. 6) subject to monitoring by the European Commission.

- *Modus operandi:* The free flow of data regulation does not provide any guidance as to velocity and method but proposes that "the detailed information and operational requirements for data porting should be defined by market players through self-regulation, encouraged, facilitated and monitored by the Commission, in the form of Union codes of conduct which might include model contractual terms and conditions."

Canada

Currently, Canadian law does not contain a general right to data portability. However, Canadians have the right to obtain access to their personal information under both of Canada's federal privacy statutes. Under the Privacy Act, the federal public sector privacy law, Canadians have a right of access to information held by government institutions.[46] As of July 2022, this right of access will be extended to any individual regardless of nationality or location. Under the Personal Information Protection and Electronic Documents Act (PIPEDA), the federal private sector privacy law, Canadians have a right of access to information held by private sector organisations covered by the law. In May 2019, the Canadian government published "Canada's Digital Charter", which contains ten principles intended to guide the federal government's work on data and digital economy policy. One principle, "Transparency, Portability and Interoperability", promotes a right to "clear and manageable access to … personal data and … to share or transfer it without undue burden" (Government of Canada, 2019).[47] The former Digital Charter Implementation Act, 2020[48], tabled in November 2020, proposed to enact a new Consumer Privacy Protection Act (CPPA) to replace Part 1 of the existing PIPEDA.[49] The CPPA would have included a right to data "mobility" that would have been enabled through regulations.[50]

At the provincial level, Quebec has recently introduced Bill 64, which proposes amendments to the Quebec Private Sector Act, including by inserting a data portability right similar to article 20 of the GDPR.[51]

- *Type of data ported*: Bill 64 relates to the porting of personal information only. Personal information held by the data holder would need to be provided "in the form of a written and intelligible

transcript… [or for computerised personal information] in a structured, commonly used technological format".

- *Beneficiary and addressee*: Bill 64 allows for transfers of data to either the person who made the request and about whom the personal information relates. Further, the amendments would require that the business must, upon request, communicate the personal information to "any person or body authorised by law to collect such information".

- *Sectoral or general:* Bill 64 provides a general, cross-sector data portability right.

- *Ex ante or ex post*: Bill 64 is an *ex ante* regulatory model.

- *Mandatory or voluntary*: Bill 64 provides a mandatory model as part of broader privacy and data protection regulation – businesses must comply.

- *Modus operandi*: Bill 64 does not provide details as to the velocity of the transfer or other details about the modus operandi.

Brazil's General Data Protection Law – Lei Geral de Proteção de Dados Pessoais

Brazil enacted a General Data Protection Law in 2018 (LGPD, being the Portuguese acronym for *Lei Geral de Proteção de Dados Pessoais*).

- *Beneficiary*: One of its greatest innovations is the broad right to data portability, which allows consumers to request an entire copy of their data in an interoperable format, which they can then take to competitors. According to Art. 18(2) LGPD, the data subject has a right to access his or her data, which corresponds to a right to be informed about such data. Art. 18(5) LGPD grants a right to data portability, which is imported from Article 20 of the GDPR.

- *Addressees and sectoral scope*: The LGPD is a cross-sectoral privacy protection regulation and thus applies across sectors.

- *Data type*: Art. 18(5) LGPD applies to both data provided by the data subject and observed data.

- *Modus operandi*: Art. 18(5) LGPD gives the right to "portability of the data to another service or product provider, by means of an express request and subject to commercial and industrial secrecy, pursuant to the regulation of the controlling agency". One of the major differences to Art. 20 of the GDPR is that the LGPD does not establish a major threshold that requires the specific consent of the data subject. For the LGPD, the request to data portability does not have to be based on an existing contractual relation to request this right from a data controller, as long as this is technically feasible. Further, the LGPD does not establish an exemption to exercise this right when the processing of personal data is necessary to perform a task carried out in the public interest or in the exercise of an official authority vested in the controller.

Singapore's data portability obligation:

Singapore's Personal Data Protection Commission (PDPC) has introduced a new data portability obligation in its Personal Data Protection Act ("PDPA").

- *Addressees and sectoral scope*: The data portability obligation applied to organisations covered by the PDPA's data protection provisions.

- *Data type*: Under the new obligation, "an organisation must, at the request of the individual, transmit personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format" (PDPC's May 2020 Data Portability Public Consultation). Singapore scopes the data portability obligation to the following: user provided data and user activity data held in electronic form (excluding derived personal data) and it applies only to data categories to be prescribed in regulations issued by the PDPC (PDPC's May 2020 Data Portability Public Consultation).

- *Modus operandi*: Singapore's initiative does not require a data controller to transmit data to the data subjects themselves. While organisations would be required to transmit data to recipient organisations based in Singapore, transmission to overseas organisations would be voluntary. However, "PDPC may also extend data portability to like-minded jurisdictions with comparable protection and reciprocal arrangements" in future.

- *Mandatory or voluntary*: The PDPA has a comprehensive review process in place, such that it has the power to review an organisation's i) refusal to port data; ii) failure to port data within a reasonable time; and iii) fees for porting data, pursuant to an individual's data porting request. The mandatory data portability requirement was passed by Singapore's Parliament in November 2020 and will be enforced once subsequent regulations are issued.

Selected private sector initiatives

The Data Transfer Project (DTP)

Since 2017, Google, Facebook, Microsoft, Apple and Twitter have joined forces in a new standard-setting initiative for data portability called the Data Transfer Project (DTP), most likely in anticipation of the GDPR Right to Data Portability (DTP, n.d.[118]; Github, n.d.[119]; Microsoft et al., 2019[120]).

The DTP was launched in 2018 as an open-source, service-to-service data portability platform so that "all individuals across the web could easily move their data between online service providers whenever they want". The DTP was motivated by the recognition that "portability and interoperability are central to innovation". In particular, the DTP aims to enhance the data portability ecosystem by reducing the infrastructure burden on both providers as well as users, with a goal to increase the number of services that provide portability.

The DTP uses services' existing APIs and authorisation mechanisms to access data. It then uses service-specific adapters to transfer those data into a common format, and then back into the new service's API. In particular, the terms of each organisation's API determine the data types that may be transferred between the providers. Overall, this includes data stored in a specific user's account. However, depending on the organisations involved, it may not be necessarily limited to that specific type of data. Use cases for the DTP include porting data directly between services such as for "i) trying out a new service; ii) leaving a service; iii) backing up your data".

MyData Global

MyData Global is a non-profit organisation with over 90 organisational members and over 600 individual members from over 40 countries on 6 continents that aims "to empower individuals by improving their right to self-determination regarding their personal data" (MyData Global, n.d.[121]). It promotes a model in which a "human-centric paradigm is aimed at a fair, sustainable and prosperous digital society, where the sharing of personal data is based on trust as well as balanced and fair relationship between individuals and organisations". The "Declaration of MyData Principles" includes a set of voluntary principles for data portability. Two points can be highlighted here:

- *Type of data*: The primary goal of MyData Global is to empower individuals to use their personal data to their own ends, and to securely share them under their own terms. Therefore, MyData Global focuses on "all personal data regardless of the legal basis (contract, consent, legitimate interest, etc.) of data collection, with possible exceptions for enriched data".

- *Modus operandi:* MyData Global aims to "empower individuals to effectively port their personal data, both by downloading it to their personal devices, and by transmitting it to other services … securely and easily, in a structured, commonly used and machine-readable format".

Data portability 3.0: Real-time continuous data transfers enabling interoperability of digital services

Early sectoral developments in the United States: From data portability 1.0 to 3.0

The Obama Administration launched a series of "My Data" initiatives from 2010 to give consumers more control over their personal health, energy,[52] finance or education data.[53] These started as data portability 1.0 initiatives as they were limited to enabling users to access and download or print their personal data with a "click of a simple button". One such initiative was "Blue Button", which was launched in the context of the health care system.

- *Beneficiaries and the type of data*: The objective of "Blue Button" was to allow patients to better access their medical records on line so they can track their health, correct errors and transfer information between health care providers.[54] Over 150 million Americans can access their health data for free in a comprehensible form, in part due to financial incentives available from the federal government to encourage providers to adopt electronic health records.[55]

- *Addressees and sectoral scope*: "Blue Button" supported the coming together of public and private sector organisations on the health care system in the United States, including federal agencies (the Departments of Defense, Health and Human Services, and Veterans Affairs). Over roughly five years, approximately 16 000 health care organisations and providers (a majority of those in the United States) signed up to the voluntary Blue Button programme.[56]

- *Modus operandi*: Blue Button was initially implemented to give veterans the ability to download or print their personal health records with a click of "a simple blue button". The Department of Veterans Affairs and the Center for Medicare and Medicaid Services under the Department of Health and Human Services were the first to offer Blue Button downloads to veterans and to Medicare beneficiaries. Two years later, in 2012, the Automate Blue Button Initiative (which provided the basis for Blue Button+) was introduced to standardise data formats and automate data transfer mechanism to enable data transfers between health data-holding organisations, patients and authorised third parties, effectively making Blue Button a data portability 2.0 initiative (Graham-Jones and Panchadsaram, 5 February 2013[122]). In 2018, the Blue Button 2.0 Implementation Guide was introduced. It defines an API standard for the transfer of "a variety of information about a beneficiary's health, including type of Medicare coverage, drug prescriptions, primary care treatment and cost" (Center for Medicare and Medicaid Services, 2018[123]). This new standard enables developers to register a beneficiary-facing application, a beneficiary to grant an application access to four years of their data and effectively makes Blue Button 2.0 a data portability 3.0 as defined in this report.

Japan's Banking Act

An amendment of the Banking Act in 2017 in Japan, which takes a voluntary approach, requires that banks disclose their terms and conditions to Electronic Payment Service providers (EPSPs) and do not discriminate against certain EPSPs. The Act also requires that third-party service providers that receive customers' banking data should have relevant measures to protect such sensitive data. On the other hand, the amendment requires EPSPs to register with the regulatory authority and to make only relevant use and management of depositors' banking information. It also sets up an amicable dispute resolution system for disputes between EPSPs and their customers. A co-regulatory approach was used to develop technical standards for the open banking APIs and the model contract between a bank and EPSPs.

- *Types of data ported:* At the request of users, the EPSPs transmit depositors' transactions or account inquiries to their banks through a digital platform.
- *Beneficiary and addressee:* Considering the accelerated trend overseas that innovative services emerged from the combination of financial service and digital technologies, the amendment of the Banking Act in 2017 was introduced to create a regulatory environment where financial institutions can collaborate with fintech firms for innovation, while ensuring consumer protection.
- *Sectors:* The amendment applies to depositary financial institutions (banks) and fintech firms that need to be registered to the Japanese financial authorities as EPSPs.
- *Ex ante or ex post:* The regulation requires *ex ante* registrations and organisational and security measures for EPSPs and banks, while the authority has the regulatory power to ask for a report, impose remedial measures, etc.
- *Mandatory or voluntary:* The amendment does not require banks to use the open APIs. Despite its voluntary approach, 72% of banks (100% for Japan domiciled banks) accepted the implementation.
- *Modus operandi:* Despite the voluntary nature of the initiative, at the time of September 2019, 95% banks (100% for Japan domiciled banks) accepted the implementation of open API.[57]

Payment Service Directive for Payment Businesses in the EU (PSD2)

PSD2, established in November 2015, sets out the rules concerning strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud; the transparency of conditions and information requirements for payment services; and the rights and obligations of users and providers of payment services. It also requires payment service providers, including banks, to allow a third party (payment initiation service providers or account information service providers) to access their customers' account data and data used for payment transactions subject to the explicit consent by the customers.[58] [59] Because of the nature of the EU directive, implementation depends on member countries. For example, in the United Kingdom, after a market research and consultation process, the CMA released the Retail Banking Market Investigation Order 2017. This requires nine major banks to set up an entity to create and co-ordinate common banking data exchange standards, including Open APIs that meet PSD2, as well as to release personal and business accounts data by January 2018.[60] OBIE designs specifications for the APIs that banks and data recipients use to communicate. It was set up by the CMA, receiving funding from the UK's nine largest banks and building societies.[61]

- *Types of data ported:* PSD2 allows third parties to access payment service providers' account data and the data used for payment transactions. Beyond this regulatory requirement, the directive triggered the commercial-based portability via APIs of other kinds of data such as identity authentication, credit scoring, trading of foreign exchange and data on loyalty programmes.

- *Beneficiary and addressee:* PSD2 aims to put in place comprehensive rules for payments services to open up payment markets to new entrants leading to more competition, greater choices and better prices for customers.

- *Sectors:* The directive applies to payment service providers.

- *Ex ante or ex post:* Requirements of the directive for data access and transfer, as well as other obligations, are *ex ante*, while the directive and related legal instruments require competent authorities' *ex post* enforcement power over payment service providers.

- *Mandatory or voluntary:* Third-party access to account data and the data used for payment transaction is mandatory.

- *Modus operandi:* Real-time data transfer is enabled via open APIs.

Interoperability in Estonia – X-Road

E-government initiatives that aim to create data exchange platforms have also facilitated data portability. One example comes from Estonia, where the government has embarked on a large-scale "e-Estonia" initiative to integrate different organisational and information systems.[62] Underpinning that initiative is "X-Road" (or "X-tee"), which is a data exchange layer technology that facilitates secure transfer of data between different information systems.

- *Addressees and sectoral scope*: Organisations can join X-tee if they clear certain security thresholds and enter into an agreement with a suitable X-tee service provider.

- *Modus operandi:* Joining X-tee makes an organisation part of an interoperable ecosystem with the technical ability to share data among other participants per the agreement.[63] International standards and protocols are used as much as possible under X-tee to ensure availability and standardisation.

The Australian consumer data right:

In August 2019, the Australian Parliament passed legislation introducing a Consumer Data Right (CDR), enabling consumers in designated sectors of the Australian economy (a "CDR consumer") to have certain information disclosed to them or to accredited persons.[64] In this way, the regime encourages innovation from providers seeking new clients. However, in the OECD Expert Consultation, Andrew Stevens stressed the importance of establishing rules and standards to facilitate interoperability (Australia's data standards were developed as open source on GitHub, with over 700 contributors from around the world), and of implementing cross-sector data portability initiatives to further innovation.

- *Types of data ported:* The right applies in respect of "CDR data", which is intended to include information relating to the CDR consumer or information that is about goods or services in a particular sector that does not relate to any identifiable consumer. The precise scope of CDR data is defined in a separate instrument that contains the rules governing the consumer data right (CDR Rules). As the CDR is only active in relation to the banking sector, CDR data include data about a consumer's accounts and products with a bank, such as transaction details, payee details and account balances. These data would likely include personal data.

- *Beneficiaries and addressees:* The legislation defines three categories of actors: i) data holders, who are the original holders of CDR data; ii) CDR consumers, who can be either individuals or small businesses that hold rights to access data held by data holders and direct that data be shared

with an accredited person; and iii) ADRs, who are individuals or businesses that meet a series of criteria for accreditation to be further specified in the consumer data rules. The CDR consumer, or the accredited data recipient with the CDR consumer's consent, can request a data transfer.

- *Sectoral or general:* The CDR is sector-specific. The legislation confers on the Treasurer of Australia an ongoing power to designate sectors of the economy that are subject to the CDR [s 56AC]. The right has commenced in the banking sector and is planned to progressively extend to other sectors, including energy and telecommunications.

- *Ex ante or ex post:* The CDR is *ex ante* regulation.

- *Voluntary or mandatory*: The CDR is entirely optional to the consumer, and there is no value generated by the regime until or unless the consumer accepts a superior offer from a banking services provider.

- *Velocity and modus operandi*: The CDR Rules do not specify the time frame in which the data must be provided in response to the request. However, failing to disclose requested data without good reason (as set out in the CDR Rules) may give rise to a civil penalty order. The CDR is flexible as to period for which data can be ported: consumers can authorise either a one-off transfer, or multiple or continuous transfers over 12 months but can withdraw their consent at any time. While the CDR Rules and Data Standards provide detailed guidance as to what information must be provided and how data should be structured, there is also flexibility as to how data are transferred. API appears to be the dominant method.

Selected private sector initiatives

Solid – towards a decentralised data web

In the private sector, Sir Tim Berners-Lee (inventor of the World Wide Web) launched a mid-course correction to the Web (named Solid) with an aim to bring user data securely together into a decentralised data store (Solid, n.d.[124]). Solid provides users an opportunity to bring data together into a decentralised data store, called a "Pod". The Pod acts like a personal web server for the user's data, with numerous benefits:

- Any kind of data may be stored in the Pod and the user can control that data. In particular, the user may determine who or what can access the data at a granular level using Solid's authentication and authorisation systems.

- The data are stored and accessed using open, standard and interoperable data formats and protocols.

- Any kind of information may be shared in the Pod.

- Users may share the slices of their data with people, applications and organisations that they select, and may revoke the access any time.

Since everything is interoperable, various applications may read and write the same data, instead of creating new data silos that may make the data difficult to use in their entirety. Overall, users have more opportunities with their data because their selected applications may access a wider and more diverse set of information. The technology of Solid has already been applied in a number of cases with an aim for users to control their data and extract value from it.

Annex B: OECD Questionnaire on data portability measures of selected online platforms

Background

Building on the findings of OECD work on *Enhancing Access to and Sharing of Data* and *Online Platforms*, the Organisation for Economic Co-operation and Development (OECD) started to work on *Data Portability* in 2019. The project will assess the role of data portability for empowering users and fostering competition and innovation, with a focus on major issues still faced by stakeholders.

It will seek to address concerns regarding identity management; privacy and data protection; security; the role of Application Programming Interfaces (APIs) and standards for data transfers (interoperability); costs; and the impact on consumers.

The main output of the project on *Data Portability* will be an OECD analytical report to be completed by the end of 2020 and published in early 2021.

Questions

Please note that these are open-ended questions. Feel free to provide as much information as possible.

- Please provide the name and e-mail address of the person completing this survey:
- **Q1.** What kind of data can be made available for data portability on your platform(s)? In case your company operates multiple platforms, please specify separately for each platform.[65]
- **Q2.** What are the three most significant challenges your company faces when implementing data portability requirements?
- **Q3.** What do you consider governments should do (or not do) as they set out to develop standards and requirements for data portability?
- **Q4.** Do you implement data portability requirements across all jurisdictions of your business locations?
- **Q5.** What are your major challenges in importing data from other online platforms?
- **Q6.** How do you facilitate data portability for your users/clients?
- **Q7.** What specific measures do you take in your data portability initiative to protect users from privacy and security risks that can arise from data transfers?
- **Q8.** Do you, if at all, co-ordinate the development and implementation of your data portability initiative with other online platforms to ensure interoperability?

Notes

[1] These characteristics include positive (in the sense that the networks become more useful as more users join them) direct and indirect network effects, cross-subsidisation, scale without mass potentially global reach, panoramic scope, generation and use of a broad set of user data to optimise their services, disruptive innovation, switching costs and, in some markets, winner-take-all or winner-take-most tendencies (OECD, 2015[34]).

[2] As noted in [C(2021)42]: "although the Privacy Guidelines already provide for many protections for data subjects under the individual participation principle, additional work is needed to clarify the application of the Privacy Guidelines to specific developments in the privacy and personal data protection sphere. These include in particular work to strengthen data subject rights (such as the right to data portability, right to correction and erasure, right to object to automated decision making) for which no clear direction has as yet emerged as to what changes or additional guidance, may be needed for such rights to be adequately addressed by the Privacy Guidelines."

[3] The summaries of the discussion at these events are available on ONE [DSTI/CDEP/DGP(2020)13; DSTI/CDEP/DGP(2021)2].

[4] Online platforms are defined as a "digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet" (OECD, 2019[1]).

[5] The 12 companies were: Airbnb, Alibaba, Amazon, Apple, Baidu, BlaBlaCar, Facebook, Freelance, Google, MercadoLibre, Rakuten and Tencent.

[6] The term "data holder" is used in this report as the more generic term to "data controller". The latter is reserved for data holders of personal data in line with the definition of the (OECD, 2013[3]) Privacy Guidelines: "'data controller' means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf".

[7] Some more detailed elements of the modus operandi, which relates to the velocity of the data transfer, include specific technical, financial, legal or organisational access and sharing requirements. Examples include the cost of access (the extent to which access is provided for free or for a fee) and the delay of execution (the maximum time foreseen by law to initiate or complete the data transfer); or the institutional arrangements (the required or encouraged involvement of trusted third parties); as well as the allowed exceptions, such as vexatious or disproportionately burdensome requests or where complying with the request would adversely affect the rights and freedoms of others.

[8] The question was: “What kind of data can be made available for data portability on your platform(s)? In case your company operates multiple platforms, please specify separately for each platform. The question accounts for the fact that some companies operate multiple platforms.”

[9] There are different types of APIs. “Open” APIs facilitate interoperability with third parties, generally by giving them access to specific datasets. Conversely, “closed” APIs are accessible only to those working within a firm, and used for integration and data sharing between teams and departments. There are also at least two types of “web APIs”: a browser API (built into the browser, allowing the user to implement functionality more easily) and a third party API (which can be retrieved from a third party to facilitate interoperability between the websites). The classification of different types of APIs is beyond the scope of this report.

[10] See Q6 (How do you facilitate data portability for your users/clients?) in the Annex.

[11] However, the right to portability in its simplest form (see Data Portability 1.0) does not require implementation of an API.

[12] See, for example, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users’ rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108, 24.4.2002, p. 51–77), preamble at (1). Article 30 of that directive contains the right of number portability. It provides that member states shall ensure all subscribers of publicly available telephone services can retain their number independently of the service and location.

[13] The Current Account Switch Service (CASS) was launched in September 2013. It is a voluntary scheme set up as part of an industry wide programme by the Payments Council and owned and operated by Bacs Payment Schemes Ltd (Bacs). It makes switching current accounts simpler and quicker for customers.

[14] The Retail Banking Market Investigation Order 2017 in the United Kingdom requires the nine major banks to set up an entity to create and co-ordinate common banking data exchange standards including Open APIs that meet PSD2 (the second Payment Services Directive in the European Union), as well as release personal and business accounts data by January 2018.

[15] Swire and Lagos’s critique applies to the draft regulation proposed by the European Commission in 2012. In the meanwhile, the regulation was approved in 2016 with modifications, which may partially address some of the authors’ concerns.

[16] Trade initiatives such as the Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore, for example, include some commitments to support development of “safe and secure cross-border electronic payments” by adopting internationally accepted standards and promoting interoperability” (OECD, 2021[138]). More specifically, “the DEPA is the first trade agreement to promote open banking through the voluntary use of open Application Programming Interfaces (APIs)” (Gallaher, 2020[142]).

[17]A data breach is “a loss, unauthorised access to or disclosure of personal data as a result of a failure of the organisation to effectively safeguard the data” (OECD, 2019[35]).

[18] This risk becomes apparent when considering Nissenbaum’s (2004[143]) concept of privacy as contextual integrity.

[19] “FTC said that the makers of the Flo app shared users’ personal health information with marketing and analytics companies like Facebook and Google – even though it had promised users to keep this sensitive information private. As part of the settlement, Flo Health, Inc. has agreed to get users’ consent before it

can share their information in the future. The settlement also requires Flo to get an outside review of the honesty of its privacy promises" (Plant, 13 January 2021[141]).

[20] See Individual Participation Principle of the (OECD, 2013[4]) Privacy Guidelines, which states that "Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them…".

[21] The survey results aim to support policy makers in determining whether and to what extent attitudes and approaches to data portability by the private sector and regulators align.

[22] The Australian Consumer Data Right in the banking sector, for example, falls within the ambit of banking and privacy regulators, including the Australian Prudential Regulation Authority, the prudential regulator of the Australian financial services industry; the Australian Securities and Investments Commission, which regulates the conduct of financial service and consumer credit providers; the Reserve Bank of Australia, the primary regulator of the payments system; the Australian Competition and Consumer Commission, which regulates competition; and the Office of the Australian Information Commissioner, which protects the privacy of individuals and handles privacy complaints (Australian Government, Department of Treasury, 2017, p. 16[79]).

[23] Article 12, paragraph 6, of the GDPR, for example, states that "Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject."

[24] See Question 7 (What specific measures do you take in your data portability initiative to protect users from privacy and security risks that can arise from data transfers?) in Annex B.

[25] The ICO recommends the adoption of current standards such as FIPS 140-2, FIPS 197 and products certified by the National Cyber Security Centre or CAPS scheme. (OECD, 2015[34]).

[26] Particular attention must be paid to the chronology of the exercise of rights. In this regard, if the request for data erasure were to precede the request for data portability, the latter would in all likelihood be compromised. Furthermore, it is quite possible to continue using a service after requesting data portability.

[27] In the case of a joint bank account, all account holders would have to be notified of each data portability request and action taken and would need to have the ability to stop a transfer at any time.

[28] See Question 2 (What are the three most significant challenges your company faces when implementing data portability requirements?) in Annex B.

[29] Sections 56BN and 56BO relate to misleading and deceptive conduct in relation to making a request. Section 56CC and 56CD relate to holding out status as an accredited body. Section 56GC provides the general immunity provision.

[30] Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features. Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[31] Section 53EO provides a civil penalty provision for failure to do so.

[32] In this context, the GDPR right to data portability concerns the data provided by users, on the basis of their consent or of a contract as also mentioned above; IPR issues may be less frequently encountered.

[33] However, the Working Party also notes that data controllers are not required to retain entire datasets for the purpose of responding to data portability requests, such that, presumably, the data controller only needs to transfer the data it has (OECD, 2015[34]).

[34] Section 56EN.

[35] The guideline refers to Recital 21 of the EU PSI Directive 2013/37/EU (EU, 2013[140]) which defines "machine readable". Directive 2013/37/EU was repealed by the EU Directive 2019/1024 on Open data and the re-use of public sector information (EU, 2019[139]) and "machine readable" is now defined as "a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it. Data encoded in files that are structured in a machine-readable format should be considered to be machine-readable data. A machine-readable format can be open or proprietary. They can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should, where possible and appropriate, encourage the use of a Union or internationally recognised open, machine-readable format. The European interoperability framework should be taken into account, where applicable, when designing technical solutions for the re-use of documents."

[36] See Question 5 in Annex B on **"**What are your major challenges in importing data from other online platforms?"

[37] The OBIE, for example, also operates the OBIE Directory, which is the trust framework central to open banking in the United Kingdom.

[38] The Berlin Group consists of around 26 banks and associations from 10 different euro-zone countries in addition to the United Kingdom, Sweden, Denmark, Norway, Iceland, Turkey, Bulgaria, Hungary, the Russian Federation, Serbia and Switzerland.

[39] These costs range from GBP 0.2-0.3 per customer (up to GBP 5 million per business) for large businesses and up to GBP 2.0 per customer (up to GBP 0.1 million per business) for small businesses in the retail sector, GBP 0.06 per customer (up to GBP 1 million per business) for large businesses in the banking sector, GBP 0.03 per customer (up to GBP 0.25 million per business) for large businesses in the energy sector, to up to GBP 0.23 per customer (up to GBP 2 million per business) for large businesses in the post-pay mobile phone sector.

[40] These costs are estimated to be up to GBP 0.06 per customer (up to GBP 2 million per business) for large businesses and up to GBP 0.70 per customer (up to GBP 0.1 million per business) for small businesses in retail sector, up to GBP 0.03 per customer (up to GBP 0.5 million per business) for large businesses in the banking sector, GBP 0.02-0.04 per customer (up to GBP 0.25 million per business) for large businesses in the energy sector, and up to GBP 0.02 per customer (up to GBP 0.25 million per business) for large businesses in the post-pay mobile phones sector.

[41] Similar findings, although with difference in the overall costs among various types of businesses, resulted from the survey on the implementation cost of PSD2 Directive for the banking sector in Poland (KPMG, 2019). Among banks, 52% said they needed more than PLN 5 million in investments to comply with PSD2, while 42% indicated a need of PLN 1-5 million and 6% less than PLN 1 million.

[42] See Sections 89-91 of (Goverment of the United Kingdom, 2013[112]), dealing with "supply of consumer data".

[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995), Art. 12.

[44] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018).

[45] Communication from the Commission to the European Parliament and the Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (COM/2019/250 final).

[46] Privacy Act, Government of Canada, 1985. Available at https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

[47] Government of Canada, *Canada's Digital Charter: Trust in a digital world*, 2021. Available at https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

[48] Government of Canada, *Modernizing Canada's Privacy Act – Online Public Consultation*, 2021. Available at https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/opc-cpl.html

[49] Parliament of Canada, *Bill C-11*, 2020. Available at https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading#ID0E0WB0BA

[50] As a result of the Canadian federal election on 20 September 2021, the proposed legislation did not go forward.

[51] National Assembly of Quebec, *Project de loi nº 64*, 2020. Available at: http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html.

[52] Another My Data initiative, "Green Button", allows utility customers to download their energy usage information in a consumer- and machine-friendly format. Launched in January 2012, the initiative is designed to promote competition and innovation among industry players. Over 50 utilities and electricity providers have signed onto the initiative (with more having pledged to join in time), allowing some 60 million homes and businesses to be able to download their usage data (see www.energy.gov/data/green-button). Both the Blue Button and Green Button initiatives focus more on providing data subjects with the right to access their data, rather than on their ability to request a data controller to share it with another controller. Both initiatives are voluntary for organisations to join, which is a significant difference from enforceable regulations like the GDPR.

[53] See further, The White House, President Barack Obama, *My Data: Empowering All Americans with Personal Data Access* (15 March 2016), available at <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access> [accessed 3 October 2019].

[54] See further Health IT, *Blue Button* (8 April 2019), available at <https://www.healthit.gov/topic/health-it-initiatives/blue-button> [accessed 3 October 2019].

[55] https://www.healthit.gov/topic/health-it-initiatives/blue-button/frequently-asked-questions and https://www.healthit.gov/topic/health-it-initiatives/blue-button/logo-and-usage

[56] See further, The White House, President Barack Obama, *My Data: Empowering All Americans with Personal Data Access* (15 March 2016), available at <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access> [accessed 3 October 2019].

[57] https://www.fsa.go.jp/singi/kessai_kanmin/siryou/20191223/05.pdf

[58] https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

[59] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

[60]https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf

[61] https://www.openbanking.org.uk/about-us/

[62] https://e-estonia.com/solutions/interoperability-services/x-road/

[63] https://www.ria.ee/en/state-information-system/x-tee.html

[64] *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth).

[65] The questions account for the fact that some companies operate multiple platforms.