International Working Group

on Data Protection

in Technology

Working Paper

The Case for Data Portability as a Privacy Protection in the Digital Age

Written procedure prior to 67th (virtual) meeting on 24 April 2021

Over the last twenty years, technology has advanced to the point where the scale of data collection and use may call for new principles in data protection and privacy law. As the OECD observed in the 2013 Privacy Framework: 1

> In the 30 years since the [OECD Privacy] Guidelines were adopted … there have been dramatic changes in the volume and uses of personal data, triggered in part by improvements in the ability to collect, store, process, aggregate, link, analyse, and transfer vast quantities of data.

The dramatic opportunities enabled by changes in technologies and global flows have also raised new challenges and concerns for individuals, organisations and society with respect to the protection of privacy.

There is a concern among some observers that privacy principles are being tested on many fronts and that the approaches taken to date may not be sufficient to respond to future challenges.

The exponential increase in digitisation is now having a broader impact both on individual autonomy and on competition within markets. This may lessen individual access to and autonomy over their own information. Data portability is the principle that individuals should be able to both directly access and require transfer of some or all personal data, in a reusable digital form. It may be one solution to address or mitigate issues related to individual autonomy and access rights.

This paper provides a first-principles approach to data portability. It explores the concept and its relationship to other recognised privacy and data protection concepts. As a first-principles paper, it

aims to avoid specific policy approaches, terminology and provisions such as the European Union's adoption of data portability in Article 20 of the General Data Protection Regulation. It does however draw on existing EU analysis, examples and guidance as well as relevant insights from other countries such as Australia's current implementation of the Consumer Data Right.

1 http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf p 66

This paper approaches data portability from a privacy and data protection perspective, noting there may be flow-on effects on competition and benefits for consumers resulting from a data portability implementation.

1. Terminology, definitions and extent of data portability

1.1 Personal data

Privacy and data protection laws and agencies across different jurisdictions refer to data access rights in various ways. The EU GDPR, the Singapore Data Protection Act, the Hong Kong China Personal Data (Privacy) Ordinance, and other jurisdictions refer to "personal data" and the "data subject", while the New Zealand and Australian Privacy Acts and others such as the Philippines legislators use the term "personal information" about an identified (or identifiable) individual. The scope and extent of this information in various jurisdictions may also vary. This paper uses the term "personal data" as a generic term to reflect what is variously described as data about a data subject, personal information about an identifiable individual, and so on.

1.2 Data portability

Data portability provides individuals with the right to request:

a) Access to [some or all] their own data; or

b) The transfer of [some or all] their data to a third party;

c)

In a re-usable digital form.

Data portability has similarities with access rights. The aspect of data portability which provides an

individual with the right to access their own data in a reusable digital form can be viewed as an extension of, or overlap with, access rights. Unlike access, however, data portability creates a new right of transfer. It also requires information to be re-usable. The right to access already requires data to be provided in a form that is readily intelligible,2 but if that information is difficult or impossible to re-use, particularly where digital collection has resulted in a plethora of data, the individual's autonomy is lessened. Data portability seeks to address that loss of autonomy and control to ensure the individual can switch to a different service provider without losing their data.

1.3 Extent of data covered by the right to portability

Data access rights usually entitle an individual to request all personal data an organisation holds about them. This is regardless of whether they originally provided the data to the data controller or it is observed data about them (or provided by a third party).

Regulators developing a data portability principle need to consider whether data portability should cover the same scope as this access right, or whether the data subject to portability requirements should be wider or narrower in scope. For example, GDPR Article 20 sets a narrower scope for data

2 See for example the OECD Privacy Guidelines.

covered by data portability than for general subject access rights. While subject access covers all personal data, the right to data portability is only for data that meets three requirements:

- the individual has provided the data;
- the processing is based on consent or contractual requirements; and
- the processing is carried out by automated means.

The Article 29 Working Party has interpreted Article 20 broadly. It issued guidelines which stated that "the right to data portability covers data provided knowingly and actively by the data subject"

but that “to give its full value to this new right, “provided by” should also include the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities.”

However, inferred and derived data are created by the data controller based on the data provided by the subject and are not covered by the GDPR data portability right. For example, a user profile created by analysis of the raw data observed or directly provided as input, such as a user profile created by analysis of the raw smart metering data collected, would not fall within scope. This information may be part of a profile about the user, but is not required to be transferred at the user’s request. It may however be required if a user makes an access request rather than a portability request, or requests information about automated decision-making or profiling.

The right to data portability as defined by the GDPR therefore does not encompass two important sets of data:3

- user profiles (patterns, preferences, scores) – because they are established by the platform provider as a result of analysis of user behaviour, rather than being provided by the data subject; and
- online ratings – because they are provided by other users, not the data subject.

The Working Group notes that including observed data in the scope of data portability will better provide individuals with control and autonomy over their own information: “the data subject will also be able to get a better view of the implementation choices made by data controller as to the scope of observed data and will be in a better situation to choose what data he or she is willing to provide to get a similar service, and be aware of the extent to which his or her right to privacy is respected.”

Some commentators consider that while GDPR Article 20 is adequate for competition purposes, to provide consumers with data empowerment it would need to extend to data provided by consumers through consumer tracking and smart devices.4

Conversely, if data portability exists as much to provide consumer benefits in the competition sphere

as to provide individual autonomy and data empowerment, then defining it according to or more

3 https://www.jipitec.eu/issues/jipitec-8-1-2017/4532 at 3.5.3

4 https://www.jipitec.eu/issues/jipitec-8-1-2017/4532 at 3.5.1

narrowly than the scope of the existing data access right may not be appropriate and may not address the problem.

The GDPR Article 20 also limits the right to apply only where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. This raises questions as to whether the generic right ought to be limited similarly, or whether it could be extended to cover other situations.

The Article 20 right is the first implementation of data portability into a privacy law. The discussion of the scope and extent to which data portability should apply is therefore useful for other regulators to follow. It may provide helpful in decisions about how extensive a right should be implemented in other jurisdictions.

2 Data portability complements other privacy and data protection rights and furthers individual autonomy in a digital environment

The right to data portability will help to ensure that privacy rights remain meaningful in a pervasive digital environment. Data portability would join other rights contained in informational privacy protection, particularly access. The right to access personal data is a fundamental element of informational privacy protection. As noted by the OECD, “The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard.”5 Access rights provide transparency to individuals, but they also facilitate the ability for individuals to maintain autonomy over and use their own information as they choose.

The 2013 OECD Privacy Framework observed that: 6

It is increasingly difficult for individuals to understand and make choices related to the uses of their personal data… Access to modify or delete personal data can also be challenging

both for individuals to obtain and organisations to provide, given existing business models, and the volume and dissemination of data in the online environment.

This access right may diminish in usefulness if the data obtained is not provided in a reusable digital format or if services hinder the efforts of individuals to make further electronic use of the data. If for example a service provides an individual with a screenshot or PDF file of their data, this technically fulfils the access obligation but it does not permit an individual to easily re-use their own data in another form, or another provider of a similar service to use that data as the basis for providing its own services to the individual. Individuals still have access to their personal data but it is significantly more difficult to understand or contextualise that data, or to make use of it.

Data portability therefore offers a complement to access rights by strengthening users' autonomy and ability to use their own personal data, as well as giving individuals more control over transferring their own information to other services.

5 http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf p 58

6 http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf p 67

The effectiveness of the right to access is at risk in an ever-expanding digital environment. This long established and fundamental individual right diminishes in usefulness if the data obtained is not provided in a reusable digital format or if businesses hinder the efforts of individuals to make further electronic use of the data. Data portability offers a potential solution to the erosion of this right.

2.1 Data portability complements access rights by providing the right to require transfer

Data portability sits alongside personal data access rights, but it does not simply update existing privacy access rights for a digital environment. Data portability introduces the new element of requiring data transfer to another service provider7. It enables individuals to require transfer directly to a third-party organisation in an interoperable form.

Updating and expanding the individual access right by requiring simply that the data provided must be re-usable only ensures that an individual is provided directly with that data. Re-entering data

manually into another service can be a major barrier to the re-use of that data by the individual. The inability to re-enter personal data into another service essentially may result in the loss of the personal data including for example contact information, calendar history, life event history, interpersonal communications exchanges and other kinds of personally or socially relevant data which could be very difficult to recreate or restore.

The European Commission identified that the difficulty in transferring personal data essentially locks consumers in to an application or service and acts as a barrier to competition:8

“There is also no explicit right [in the usual right to access] for the individual to extract his/her own personal data (e.g. his/her photos or a list of friends) from an application or service in a format that may be processed further, so that the individual may transfer data to another application or service. With increasing use of a certain online service, the amount of personal data collected in this service becomes an obstacle for changing services, even if better, cheaper or more privacy friendly services become available…This situation effectively creates a lock-in with the specific service for the user and makes it effectively very costly or even impossible to change provider and benefit from better services available on the market.”

Data portability can enable individuals to take their transaction histories with them when they switch to a new bank, telecommunications company or internet service provider. The right would also be relevant in relation to online cloud services that provide storage and access to personal data, digital photo albums and videos. It would allow individuals to request a download of their personal data that they can carry with them to a new provider or service.

Data portability is a response to the challenges of the digital economy and particularly the increased siloing of individual information in large-scale social network platforms and other digital

7 Under the EU GDPR Art. 20 a data subject cannot require a controller to transfer data to a third-party organisation rather an individual has the right to have data transmitted directly from one controller to another controller.

8 European Commission Staff Working Paper, Impact Assessment, SEC (2012) 72 final, p.28.

conglomerates. It is a recognition of technological advancement, with a significant by-product being a potential increase in the competitiveness of relevant digital markets. It complements the existing access right by allowing an individual to make more use of their own data. It addresses the difficulty in transferring information from one service to another, which serves to keep customers locked into a particular provider's service. Individuals being able to require transfer from one service to another, rather than re-entering their own data manually, will assist in providing them with control and autonomy over their data and which service they would prefer to engage with.

2.2 Data portability promotes empowerment and autonomy

Privacy law seeks to empower individuals to maintain control over their personal data. But principles seeking to empower individuals are rendered ineffective if individuals are locked into relationships with data service providers because they cannot effectively extract personal data and seamlessly move to another provider.

Lock-in is a privacy problem as it signifies a loss of an individual's autonomy and control. It can also render illusory the meaningful exercise of the right to access one's own personal data.

. Data portability allows individuals to access their personal data in a format that enables them to re-use it. As the Australian Treasury observed in its analysis of the Consumer Data Right (Australia's implementation of data portability), the new access right granted by data portability has greater functionality, more security and may apply to different kinds of data than existing privacy rights.9

2.3 Data portability may lead to business competition improvements for consumers

Data portability empowers consumers to make choices allowing market forces to respond. When individuals sign up with a service provider they may have a choice. They might research how that provider will use their data and the services provided. As time goes by an individual may wish to switch to another provider. A new provider may offer a better service or price or the individual may have lost trust in the first provider. Individuals should be able to switch services, especially in a world

where service providers unilaterally change business models or discontinue services.

In competitive markets, consumers should be able to compare the rates and services on offer from different companies with a realistic prospect of being able to move to a new provider if desired. The threat of losing customer to competitors also encourages companies to provide better offerings to meet consumer demand.10

Reducing the friction associated with access to and movement of data, may promote the development of new and innovative product/service offerings thereby encouraging economic growth.

2.4 Data portability may also promote better privacy practices through increased competition

9 https://static.treasury.gov.au/uploads/sites/1/2018/08/Consumer_Data_Right_Privacy_T316972.pdf

10 https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability

Although the advantages in preventing consumer lock-in are strongly related to promoting effective competition, there are also interlinked privacy benefits. Data portability assists in redressing the power imbalance between consumer and provider. This means it also enables customers to move off platforms which use personal data as a currency, or to shift to more privacy-protective platforms without the attendant inconveniences or risks of significant data loss.

Facilitating customers in switching providers creates a feasible response for the consumer in situations where a data breach or policy change has undermined that consumer's trust. At a collective level, switching by many consumers as a response to poor privacy practices may encourage poor performers to improve their privacy protection. This would raise the bar as a 'race to the top' in the privacy sphere.

The ubiquity and market power of individual companies may counteract the benefits increased competition on privacy offerings could offer. Examples such as the Cambridge Analytica scandal resulted in Facebook's users' confidence in the company's commitment to protecting privacy dropping by almost 70%, according to one independent user survey.11 Survey respondents indicated

that despite their loss of trust, they were unlikely to shift services. 12 Reasons given included the effort involved in starting a new account on another social network, and the fact that other companies' privacy practices may be no better. With that said, data portability may encourage the new market entrants which innovate on the way they treat user data. However lock-in problems may arise when there are high costs associated with switching providers.

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. This may be an important right to secure and enforce against receivers or new business owners from a consumer protection perspective.

Data portability intersects and overlaps with both data protection and consumer protection and competition. Several jurisdictions that have introduced the right to portability have done so as a form of competition regulation. Australia has chosen to treat it as a competition regulation with support from data protection agencies.13 In Hong Kong, the right is also being explored by the Hong Kong Monetary Authority as a regulatory guidance framework for the banking industry.14 The Singapore PDPC has also co-developed a Discussion Paper on Data Portability with the Competition and Consumer Commission of Singapore.

As acknowledged by the Article 29 Working Party, however, while the right to data portability may enhance competition between services (including by facilitating service switching), the GDPR's

11 https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011

12 https://www.businessinsider.com.au/people-increased-facebook-usage-after-cambridge-analytica-scandal-2018-5?r=US&IR=T

13 See the EU GDPR Article 20, the Philippines Data Privacy Act 2012 section 18, and the Australian Consumer Data Right.

14 See the Consultation Paper on Open Application Programming Interfaces Framework for the Hong Kong Banking sector.

introduction of data portability is to regulate personal data and not competition.15 The Philippines and Brazil16 have also implemented data portability as a right contained within data protection law. Conversely, in France, the 2016 Digital Republic Act17 introduced a new section under the Consumers Code, which grants consumers a right to the recovery and portability of their personal data. This new provision requires all providers of online communication services to the public to enable consumers to recover, free of charge, all data that they have stored online, including data files, all data stored and accessible from the user's online account, and other types of data that are associated with the user's online account and that can be easily re-used and exploited by another data controller. The data controller must provide the data in a readable format. If that cannot be done, the data controller has to inform the consumer of such restriction and provide alternative ways for the user to recover his/her data.

Similarly, this paper approaches data portability from a privacy and data protection perspective so does not propose to explore the effects on competition or consumer benefits more than in a general sense. However, it is noted that while data portability enables elements of individuals' privacy and data protection rights, it can often fall short as an enabler of greater competition and diversity in digital markets.18

For example, Article 20 of the EU General Data Protection Regulation provides individual data subjects with a right to transfer a significant part of their data from one service to another. It is a right to obtain data in a machine-readable format. And this makes it a limited right when it comes to addressing market power. As mentioned above, that specific right is limited to the data that a user voluntarily consented to sharing with a platform, and does not provide data subjects with the ability to transfer metadata or other inferred data about them that platform owner has access to and that is a significant source of market power.19 Also, it does not entail an automatic right to have two or more competing services rendered fully compatible or interoperable, nor the ability on the part of European consumers to access a plurality of equivalent services on equal terms.

3 Policy matters to consider when adopting and implementing data portability

As signalled above, policy-makers and legislators should consider whether to implement a data portability right as:

15 Article 29 Working Party guidelines on the right to "data portability" (wp242rev.01), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

16 General Data Protection Law, federal law 13.709/2018 (LGPD)

17 Loi n°2016-1321 pour une République numérique, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id

18 https://privacyinternational.org/explainer/4130/explainer-competition-data-and-interoperability-digital-markets

19 Inge Graef, Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union, Telecommunications Policy 2015, Vol. 39, No. 6, p. 502-514.

a) a data protection right which inherently includes elements of consumer protection;

b) a form of competition regulation; or

c) a regulation which spans the two and brings both elements together.

In the latter case, privacy and data protection supervisory authorities and competition agencies would ideally work together to regulate the right as it relates to each of their respective fields.

There are various other policy options for addressing the issues data portability is intended to resolve, and which may introduce the benefits which accompany such a right. Those options include:

- a general data portability law;
- sectoral or targeted data portability laws;
- integrating aspects of portability rights into subject access laws; or

- encouragement to organisations to voluntarily offer this option, without legislating to require it.

There are also many policy issues and decisions which regulators must make in developing the general data portability right:

- how data should be provided and by which means;
- whether the right should be implemented universally or sector-by-sector (or only to specific sectors);

the extent of the right – whether it should apply only to digital or internet-based sectors, or more broadly; and

- any exceptions which should apply.

3.1 Data must be provided or transferred in a reusable electronic form

Data portability requires that one agency can transfer an individual's personal data, in an electronic format that remains usable with another agency. Rather than 'reusable', this could also be framed as 'machine-readable', 'readable', 'accessible' or 'usable'. By comparison, traditional access rights do not require that data be provided in an electronic and reusable form.

At minimum, data provided via data portability requests should be:

structured;

- machine readable; and
- provided in an interoperable format.

This element raises questions about common machine-readable formats, minimum standards for data to be ported, and transmission standards. The GDPR right entitles individuals to receive data in a 'structured, commonly used, machine-readable and interoperable format', which allows them to move, copy, or transfer personal data easily across different services. This framing includes various

specific technical terms for data storage and format. The Open Data Handbook assists with defining what these various terms mean.20

‘Structured’ data means that software must be able to extract specific elements of the data – for example, a spreadsheet where the data is organised into rows and columns. It allows for easier transfer and increased usability.

Machine readability means that the data is in a form readily processable by a computer, without human intervention, and while no semantic meaning is lost. Such data can be automatically read and processed, and the individual elements can be easily accessed. Machine-readable data can be made directly available to applications that request that data over the web, by means of an application processing interface (API). Interoperability allows different IT systems to share data and resources. An interoperable format allows data to be exchanged between different systems and be understandable to both. As the Open Data Handbook recognises, without interoperability the different systems and components cannot work together. At the same time, organisations are not expected to maintain systems that are technically compatible with those of other organisations; data portability is intended to produce interoperable systems, not compatible ones.21 The GDPR is technology-neutral and prohibits mandating any particular interoperability standards or requirements to create compatible systems.

The specific standards might differ across jurisdictions; some jurisdictions may choose to specify that data governed by data portability must be made available to API access, while others may require organisations to use a specific open format such as CSV or XML. Others may leave these unspecified. These are choices at a policy setting level and require consideration of the requirements of that country or the particular sector being regulated.

There are real practical difficulties of implementing these specifics across a sector, and the cost to business should not be underestimated (particularly if the regulatory setting requires mandatory API access or similar). Regulators will need to have regard to the timing and digital maturity of businesses within their jurisdictions. However, achieving minimum international standards will assist

in a cross-jurisdictional right allowing individuals to access their data even if the organisation is located other than in their country. For this reason regulators should be wary of setting particular requirements for their jurisdiction which may not fit into what is commonly used elsewhere.

We leave open the question of interoperability and encourage the development of standards by the industry. An organisation such as the ISO may also assist in providing guidance.

3.2 Digital-only data portability or all data

The requirement to provide personal data in a reusable electronic form raises issues as to whether the generic right to data portability should apply only to electronic data, or whether it should also

20 http://opendatahandbook.org/

21 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

include non-electronic data. The latter could create significant compliance costs for businesses in digitising their paper-based data to provide the data in a “reusable electronic form”. The right to data portability has arisen at least in part as a response to increased digitisation. Extending it to include non-electronic data such as historic paper files may not be feasible or appropriate, notwithstanding the consumer benefits in digitally unlocking this data.

3.3 Universal application or sector-by-sector application and implementation

Regulators must decide what parts of an economy the data portability right should apply to. Applying the right to the entire economy could create significant compliance costs for ‘bricks and mortar’ and very small organisations, although they may hold similar amounts of electronic data on a customer.

While the GDPR does cover government agencies, Article 20 of the GDPR provides that the right to data portability does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, i.e. it does not apply to typical processing operations in the public sector. Regulators may wish to consider whether

an extension to the public sector would be a favourable extension in future. In comparison to private agencies, however, individuals will generally not be able to request a government agency to transfer their data to another agency because of the monopoly of providers within government – for example, most jurisdictions will have only one tax department. However, in terms of consumer autonomy, it might be helpful for an individual to request that the tax department transfers their tax records to a third-party accounting provider who the individual has contracted for their accounting and tax affairs. Similarly, an individual might prefer that their information is transferred directly at their request from one social service provider to another social service provider within government (for example, from the Registrar of Births, Deaths and Marriages to another agency for the purpose of confirming a name change or identity attestation), rather than having to provide their same information to two separate government agencies. If data portability is conceptualised as a data protection right which enhances individual autonomy, empowerment, and access to/control over their own information, rather than only as a consumer/competition right, then extending it to cover government organisations may be appropriate.

Regulators will need to determine whether the right should apply to all organisations or to specific sectors, and further how implementation of the policy will take place – as a universal implementation or sector by sector. The latter is the approach Australia has taken with the Consumer Data Right, which will first apply to the banking sector under a framework known as Open Banking. The energy and telecommunications sectors will follow.22 The Australian Competition and Consumer Commission will take the lead regulator role, working closely with and supported by other organisations, particularly the Office of the Australian Information Commissioner and the Data Standards Body.23 This multi-agency approach reflects the interplay between privacy and

22 https://www.accc.gov.au/focus-areas/consumer-data-right

23 https://www.accc.gov.au/focus-areas/consumer-data-right

consumer/competition rights. The Hong Kong Open Application Programming Interfaces (API)

Framework would also be adopted to facilitate only the banking industry.

If data portability is implemented as a sector-by-sector regulation, policy-makers must also consider how to address cross-sector interactions. Particular challenges will arise where data sets are ported from a regulated sector to a non-regulated sector. This raises questions on who should bear the responsibility of accuracy for the ported data, and the challenge in scoping the data to be ported.

Countries may already have some legislative frameworks that require specific sectors or agencies to transfer personal data at the individual's request. For example, in New Zealand section 22F of the Health Act 1956 requires agencies holding health information to transfer it to anyone else providing services to the individual, if requested to do so by the individual or the third party.24 The health information cannot be withheld because payment has not been made or to avoid prejudice to a commercial position.

Regulators should also decide whether organisations which are excluded from the data portability requirement should also be excluded from receiving data ported from another organisation pursuant to the data portability requirement.

3.4 Other exceptions on data portability

Access rights in privacy and data protection law typically include a range of exceptions such as:

- security, defence;
- trade secrets; and
- disclosure of another individual's personal data.

Data portability creates particular issues relating to intellectual property, commercial sensitivity, competitive advantage and impacts to innovation, especially regarding derived or proprietary data.

Comprehensive data portability should include the profile data collected or generated about a user for marketing or advertising purposes, as well as data from third parties and inferences the company makes about a user's habits or demographic group.25

If a broad data scope is established (e.g. including data inferred about a subject) this may allow other companies to reverse-engineer proprietary algorithms and use them to replicate a service or product. A balance therefore must be reached between an individual's right to access data from and about them, with a company being able to protect their intellectual property and commercial interests. While this policy setting is one for each jurisdiction to consider, businesses rely on

24 The Health Act does not specify the form in which health data must be provided, which distinguishes it from the general data portability right. However, the Act was written prior to the significant increase in digital data. It is also likely that the health sector already involves structured data in the form of medical notes, X-rays, and so on, which will be accessible and understandable to other health professionals.

25 https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability

certainty. A bright-line test may not be appropriate, but jurisdictions do need to make clear, and enforce, the limits of which data will be included in scope.

Data portability may also involve disclosure of another person's personal data, particularly in sectors such as social media. If porting a social media account includes friends' contact information, photos, comments, and so on, this may involve privacy and security risks for those individuals. For example, Facebook users can download an archive containing their Facebook history, including information on any purchases made via Facebook including payment data, Internet Protocol addresses, details of deleted friends, and a facial recognition identifier.

The Electronic Frontier Foundation suggests that consent may be a starting point – that a service could ask a user's friends for specific, informed consent to share their contact information as part of a user-initiated download or data transfer. They also suggest that "companies should explore technical solutions that might allow users to export lists of friends in an obfuscated, privacy-protective form."26 However, using consent as a starting point may create practical problems such as notification fatigue and compliance costs.

Alternatively, this issue may reflect a broader issue in predicating the right to data portability on ‘personal data’ or ‘personal information’ as with the general data access right. It may be more appropriate to define the data within scope of data portability as consumer data: data which has been provided to or created by the company, which is about or associated with the account of the consumer. Some have even suggested introducing a new broader right to ‘identity portability’.27

4

Implementation issues

There are implementation issues that must also be considered when creating a data portability right. These include:

the security risks in data portability;

- data collection minimisation; and

the role of privacy and data protection authorities.

Conducting a Data protection impact assessment (DPIA) is recommended in order to properly assess these issues.

4.1 Security risks involved in data portability

26 https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability

27 In his policy paper Enhancing Competition with Data and Identity Portability, Joshua Gans suggests that a new, broader right of identity portability should be introduced. He notes that “a major part of platform switching costs derive from users’ provision and consumption of data that others provide” and that identity portability would allow the consumer to retain existing permissions to access data provided by others. For example, a user would be able to leave a digital platform (and therefore its algorithms and services) but continue to be able to communicate with their contacts who are still based on the platform.27 This proposal appears to address the issue of porting other users’ personal data, but may only be appropriate in a social network context.

Regulators should not overlook the security risks of transferring personal data from one service to another. The strength of data portability in making information easier to share could encourage risky information sharing, including when it might be inappropriate from a privacy perspective or when information is illegally accessed by a malicious third party.28 Data portability may also increase the potential damage when an unauthorised party gains access to an account.

Data portability presents significant security risks should organisations not port an individual's data with adequate security standards in place both during the transfer and once held by the receiving organisation. Data should always be protected with strong security in transit and at its new location with the third-party organisation.29 Both consumers and organisations should be aware of any potential risks before moving their data to another service. Risk mitigations such as a delay from when the request to transfer is made to when it is carried out, notifying a user via previously used contact methods that a transfer request has been received for their data, requiring another verification method before approving the transfer, and so on should be considered.

Ideally users should be cautious about requesting a transfer to a third party with inadequate privacy and security standards. However, relying on users to make adequate security assessments may well be too onerous a burden for the average consumer. It is possible that businesses may respond to market demand for security-protective portable offerings by marketing themselves as particularly security-conscious and therefore a 'safe' organisation with which consumers should entrust their data. Similarly, third party transfer specialists could enter the market and offer their services to companies seeking to comply with data portability requirements.

In implementing any new right to data portability, policy-makers should consider related issues regarding:

- protection of data during the transfer from an organisation to an individual;
- protection of data during an organisation to organisation transfer; and
-

the role of the receiving organisation in providing verification that the data has been received successfully.

Regulators should also consider providing guidance on where liability should fall in the case of a security or privacy breach during the transfer – whether with the transferring organisation, the recipient organisation, or both.

4.2 Incompatible data sets

Portability may also impose obligations on organisations receiving the data. Under some privacy and data protection regimes, organisations may only process data that is relevant to their purposes (i.e. a legal obligation of data minimisation and purpose limitation). This creates questions as to what a responsible organisation should do if it receives data for which it does not have a purpose.

28 https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability

29 https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability

For example, if a user requests one social networking service that hosts text, picture, and video messages to port their data to another service that only hosts video of up to six seconds, should the recipient service delete this data, or is it required to process and store it? This creates open questions as to whether the burden should fall on the user, on the sender, or on the receiver. However the receiving service should only process data that is relevant and necessary for its purposes and when it has a legal basis to do so. Organisations could potentially address this issue through technical means and/or by including in the portability section of their privacy statement a disclaimer that any ported data relating to services they do not offer will not be held, but this again requires individual users to educate themselves on each service’s privacy policy.

4.3 The role of privacy and data protection authorities

Privacy and data protection authorities will necessarily have a key role in review, oversight and compliance activities if data portability is implemented within privacy and data protection regulations. For example, privacy and data protection authorities may take on a role in reviewing

organisations' refusal to transfer data to individuals or to other organisations, similarly to existing access request complaints. Authorities may also need to respond to data breach situations where ported data security has failed.

Other issues for consideration include:

(i) regulating the time period within which organisations must provide data to the individual or transfer data to another organisation; and

(ii) whether organisations may charge individuals or receiving organisations for the transfer of personal data.

Questions will arise such as which law should apply if for example an organisation in one jurisdiction is permitted to charge for transfer, but the consumer is based in another jurisdiction where charging is not permitted.

These implementation issues will need to be determined at a policy level for each jurisdiction. However, they too will create cross-jurisdiction interoperability issues.

4.4 Interaction with the right to erasure

It is not clear how data portability interacts with the right to have data deleted by a controller which holds data once the individual is no longer using that service. Article 17 of the GDPR provides the 'right to be forgotten' in certain circumstances but this is not tied to the right to data portability.

Many privacy and data protection jurisdictions impose obligations on controllers to delete data once it is no longer necessary for the purposes for which the data was obtained. However, controllers may try to skirt this obligation regarding data portability by using broad privacy statements that cover wider uses for the data, other than the primary purposes for which it was collected (for example, for internal research and analysis). This would mean those controllers might be in breach of privacy and data protection laws if they cannot demonstrate a legal basis to use the data.

When considering a right to data portability consideration should also be given to whether a right to erasure should be established. This would mean that users can request the transfer of their data and

the deletion of their data from the first service provider once the transfer is complete. A right to erasure may be superseded by other legal obligations or clear purposes for holding data, such as public records legislation or anonymised datasets for analytics.

4.5 Competition and compliance issues

As previously signalled in the discussion of competition, data portability might create a tension between an individual's right to access their personal data and the potential commercial sensitivity of that data. This tension will be most obvious where the data to be transferred has been processed in a way that adds commercial value to the data processor (and would be of value to that processor's competitors).

A data portability right may raise the barriers to entry and increase compliance costs for businesses, especially for small/medium enterprises. This is particularly the case if businesses are required to digitise all data or ensure that their database is accessible by API to allow for data portability requirements. Large organisations may have the capacity to comply, but smaller enterprises may find this an overly onerous requirement. On the flip side, greater access to data that would otherwise have been 'locked-in' to an agency could lower barriers to entry for some new entrants and thereby invigorate competition in some markets.

4.6 Policy interoperability

A key issue to address is the relationship between the various jurisdictions with and without data portability laws, and how this should be optimised for consumers. The EU is not the only economy promoting data portability. Several other jurisdictions have provided or are considering providing for the right to data portability in various ways. As previously mentioned, the Philippines and Brazil have provided a similar right to data portability and the Australian Consumer Data Right is being implemented progressively in a sector-by-sector approach. In 2018, the Competition and Consumer Commission of Singapore and the Personal Data Protection Commission announced a joint initiative studying consumer protection, competition and personal data protection issues.30

The drafting and scope of the right in other jurisdictions may appropriately differ from the EU right.

However, the objective would be to produce a right that is interoperable with the GDPR (and any other emerging international approaches). In other words, an organisation meeting the requirements of the proposed right in another jurisdiction should thereby be confident of meeting the GDPR requirements if it was to trade into the EU. Similarly, European consumers should be able to confidently switch their data to or from an overseas provider, just as overseas consumers might benefit from the new GDPR right in dealing with an EU-based business.

5 Conclusion

The potential benefits data portability offers are significant. It would provide individuals with an enhanced right to access and control their personal data, to counter the erosion of that right

30 https://www.opengovasia.com/singapores-consumer-watchdog-announces-studies-on-data-portability-and-online-travel-booking

brought about by rapidly expanding scope and capability of digital data collection. It would also empower consumers to make choices about which services they use without fear of losing personal data because of switching.

At the same time there are many interrelated and complex policy issues to consider, both in the jurisdictional approach to data portability and in its implementation. Despite these complex considerations, data portability is a worthwhile addition to the informational privacy protection sphere. It reflects the principle of individual autonomy in informational privacy, while ensuring access and control rights remain relevant for the digital age.