Comments to the Federal Trade Commission on Data Portability

AUGUST 21, 2020

FACEBOOK

Table of Contents

Introduction

Facebook appreciates the opportunity to provide these comments as part of the Federal Trade Commission's ("FTC" or "the Commission") Workshop on Data Portability.[1] We believe that part of having a free and open internet means that people should be able to share their data with the apps or services they like most. As our CEO Mark Zuckerberg has said, if you share data with one service, you should be able to move it to another.[2] This gives people control and choice, while also promoting innovation. That's why we support the principle of data portability.

There's growing agreement among policymakers around the world that data portability can help promote innovation online and encourage the emergence of new services. However, to build portability tools people can trust and use effectively, online services need clear rules about what kinds of data should be portable and who is responsible for protecting that data as it moves to different services. Although some laws already guarantee the right to portability, our experience suggests that companies and people would benefit from additional guidance about what it means to put those rules into practice.

Last year, we published a white paper that explores these issues and the privacy questions we've encountered as we build a new generation of data portability tools.[3] Since then, we've had conversations with stakeholders around the world—from the U.S., UK, and EU to Brazil and Singapore—to get feedback about what data should be portable and how to ensure that we protect privacy when enabling data transfers.

As we have these conversations, we're continuing to develop and launch products that take into account the feedback we've received and will help drive data portability policies forward by giving people and experts real-world products to assess.

In these comments, we describe how Facebook implements data portability. We describe the history and functionality of our portability product offerings, including our participation in the Data Transfer Project and the recent launch of a product that allows people to transfer their Facebook photos and videos to other services. In the coming months, we intend to expand the scope of our data portability offerings. To that end, we also describe the wide range of considerations—including user interest, privacy, and security—that drive our portability product development.

---

[1] Federal Trade Commission, "Data to Go: An FTC Workshop on Data Portability" (Mar. 31, 2020), https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.
[2] *See* Mark Zuckerberg, *The Internet Needs New Rules. Let's Start in These Four Areas*, WASH. POST (March 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.6247ef86cd32.
[3] *See* Erin Egan, *Charting a Way Forward: Data Portability and Privacy*, FACEBOOK (Sep. 4, 2019), https://about.fb.com/news/2019/09/privacy-and-data-portability/.

We conclude by drawing the Commission's attention to the policy and regulatory tensions that surround data portability and we explore in our white paper, including questions about scope, privacy obligations, and accountability. We also highlight emerging technical and policy mechanisms to address these challenges. As the FTC and Congress evaluate existing implementations of data portability and the prospect of a comprehensive federal privacy law or portability legislation in the U.S., we urge it to keep these tensions and our recommendations in mind.

The Commission should ensure—by recommending dedicated federal portability legislation and advising industry on how to best respond to these policy and regulatory tensions—that service providers implementing data portability have the clear rules, accountability frameworks, and certainty necessary to build products that enhance people's choice and control, are easy to use, and privacy protective.

Facebook's Data Portability Products

Over the years we've developed a range of tools that allow people to easily view and download the data people have shared on our apps and data about their activities on those apps, including Download Your Information (DYI) on Facebook, Download Your Data (DYD) on Instagram, and Access Your Information (AYI). Recently we launched a new tool that allows people to transfer their Facebook photos and videos to other services, starting with Google Photos.

Download Your Information / Download Your Data

Scope

Download Your Information includes two sets of information: 1) Your Information, which includes information requesting individuals have entered, uploaded and shared on Facebook, such as their profile information, posts, likes and comments; 2) and Information About You, which includes information associated with a requesting individual's Facebook account, such as their logins to Facebook, what devices they use, and information used to make recommendations on News Feed, Watch, and News. Download Your Data includes similar categories of information for Instagram users. Access Your Information is a place on Facebook for people to find a summary of their Facebook account information that they can access at any time and in a single place.[4]

History

Download Your Information was launched in 2010, offering people the ability to download a copy of the information they have shared on their profile. In 2018, DYI was refined to allow people to 1) select individual data types to download and 2) make more granular choices about how they receive their data, such as choosing image quality and a date range to download. Access Your Information was also launched in 2018.

---

[4] *How do I view my information on Facebook?*, FACEBOOK Help Center, https://www.facebook.com/help/1700142396915814.

Since then, we've continued to update these tools to include new data based on product updates, technical ability, and additional feedback we receive from experts. Most recently, in March 2020, we added more data to these tools, including data used to improve people's experiences on our platform.[5]

Functionality

People can request their data file at any time and choose to receive it in an HTML file (DYI) or JSON (DYI and DYD).[6]

HTML is a commonly used, easy to view format of data on Facebook. People receive a .ZIP file that, once opened and extracted, will contain an .HTML file named index that they can open like a web page on their web browser. The .ZIP file will contain folders with files, including any images and videos requested. JSON is a machine-readable format of data that could allow people to transfer their information more easily when uploading it to another service.

We have a number of security measures in place to help keep accounts secure and protect information on Facebook, including in the context of DYI. Before people can begin downloading a copy of their information, we'll first ask them to re-enter their password. We may also ask people to complete additional verification steps before allowing downloads to begin. To help protect accounts, download requests will expire after a few days—people can always request a new one.

"Transfer a Copy of Your Photos and Videos"

The Data Transfer Project

In 2018, we announced our participation in the Data Transfer Project, a collaborative effort with Apple, Google, Microsoft, and Twitter to build a common way for people to transfer their data between online services.[7]

The goal of this project has been to make it easier for services of any size to securely make direct transfers for data portability from one service to another at the request of their users and to make the process simpler for the people who use these services.[8] The project does this by providing an open source library that any service can use to run and manage direct transfers on behalf of users.

---

[5] *See Updating Our Data Access Tools*, FACEBOOK (Mar. 30, 2020), https://about.fb.com/news/2020/03/data-access-tools/.
[6] *See How do I download a copy of my information on Facebook?*, FACEBOOK Help Center, https://www.facebook.com/help/212802592074644; and *see How do I access or review my data on Instagram?*, Instagram Help Center, https://help.instagram.com/181231772500920.
[7] *See generally* Steve Satterfield, *Working Together to Give People More Control of Their Data*, FACEBOOK (July 20, 2018), https://about.fb.com/news/2018/07/data-transfer-project/.
[8] *See About Us*, DATA TRANSFER PROJECT, https://datatransferproject.dev/.

The Data Transfer Project comprises three main components:

1. A set of shared data models to represent each vertical (i.e., photos, contacts, playlists)
2. Adapters, which handle the authentication of a user to a service (normally OAuth, an existing industry standard) and the transformation of data to and from the shared data models (importers and exporters)
3. A task management framework, which puts all the pieces together and handles the life cycle of a transfer job, including job creation and running the transfer

Rather than expecting every company to build its own system from scratch, this open source framework allows them to share any improvements in the framework as well as adapters and data models. For example, a company using the Data Transfer Project framework can send an existing data type to a new service by simply creating a new Data Transfer Project import adapter for that data type. The code for that new import adapter can also be contributed back to the open source project, thereby allowing other companies to build export functions to that new service, as well, with no additional technical work. Anyone is free to create their own adapters, models, and tools based on the Data Transfer Project and use it independently or to supplement their existing functionality.

The Data Transfer Project code is small enough that an individual can run it on a laptop to inspect and test, but is also easily scalable for enterprise deployments. The Data Transfer Project can be run locally in memory for testing and by individuals who want to try out the code. The service is also highly extensible, which allows it to be deployed in cloud environments and as a back-end service in enterprise-level infrastructure. There are public, open source extensions that allow the Data Transfer Project to be run on the Google Cloud Platform and Microsoft Azure cloud hosting providers. Deploying the Data Transfer Project framework at scale so that it would work seamlessly with our infrastructure-specific back-end services required thoughtful engineering and design work.

Deploying the Data Transfer Project at Facebook

Earlier this year, we announced a new tool on Facebook that allows people to transfer their data—currently, photos and videos they have uploaded to Facebook—directly to Google Photos.[9] We plan to expand this to other services in the near future. This tool is based on code developed through our participation in the Data Transfer Project, described above, and its development was informed by the feedback we received in the conversations that followed publication of our white paper on portability.

---

[9] *See* William Morland, *Data Transfer Project: Enabling portability of photos and videos between services*, FACEBOOK Engineering (Dec. 2, 2019), https://engineering.fb.com/security/data-transfer-project/.

Functionality

People can access this tool from the Facebook Settings, under "Your Facebook Information", alongside AYI, DYI, and a variety of additional controls. After selecting "Transfer a Copy of Your Photos or Videos", we ask people to verify their identity by re-entering their password. Next, they can select a destination—currently we offer Google Photos, with plans to offer additional destinations under development—and choose to transfer all of their Facebook photos or videos. People are then asked to enter their Google Photos password and confirm their desire to transfer. When the transfer is complete, people receive a notification on Facebook and via email.

Privacy & Security Considerations

Any mechanism to send data outside of a service carries risk. We examine many of these risks in our white paper on data portability and privacy. Based on feedback from the conversations that followed publication, we have put a variety of measures in place to mitigate these risks.

For example, we use the commonly-used protocol OAuth to authenticate people with the destination service. It's important that the system request only the permissions required for the task at hand. Access by the destination service should end once the transfer is complete. Finally, transfers should only be created by the owner of the account. In order to verify this, we ask people to re-enter their password before initiating a transfer. We also send an email to the registered account once a transfer has begun, which allows people a chance to stop the transfer if they change their mind or do not recognize the request.

As we and other companies build out our portability products, the privacy and security challenges will grow with them. We encourage the Commission to examine the questions and recommendations we put forward in our white paper and below to ensure that service providers have the clarity and certainty we need to build data portability at scale.

Roadmap

Our investment in the Data Transfer Project provided the technical basis for our new data portability product, "Transfer a Copy of Your Photos or Videos". We remain committed to ensuring the current product remains stable and performant for people and we are also exploring how we might extend this tool, mindful of the need to preserve the privacy of our users and the integrity of our services.

Our product decisions are not made in isolation. We're informed by user interest, policy and regulatory conversations spurred, in part, by our white paper on portability, and our participation in the Data Transfer Project to gather insights from people, policy stakeholders, and the developer community.

Given the variety of interests, equities, and risks raised by implementing data portability, our product decisions are deliberate and driven by a wide-ranging assessment[10] of where we can make the most meaningful contributions to our users, the innovation ecosystem, and society at large.

We therefore are exploring the extension of our Data Transfer Project work in three dimensions: 1) improving the reliability, performance, and user experience of the product; 2) adding new destination services for photos and video; 3) supporting new use-cases and data types.

Improving reliability, performance, and user experience

To scale our offerings, we'll need to continue to invest in the performance, reliability, and efficiency of our data portability products. Those investments provide the foundation upon which we can build a richer user experience that gives people more choice over which data they want to transfer and how.

Adding new destination services

Supporting these additional use cases will mean finding more destinations to which people can transfer their data. In the short term, we'll pursue these destination partnerships through bilateral agreements informed by user interest and expressions of interest from potential partners.

Adding new use cases and data types

Moving beyond our current use case (photo and video archival), we aim to explore new opportunities for people to derive value from porting the most widely used content on Facebook.

Some possible examples include the ability for:

- Content creators to build their brands on new platforms by transferring the media they've produced or shared on Facebook,
- Event organizers to share and track their Facebook events on cloud-based calendar services, and
- Anyone to transfer a copy of their most meaningful posts to a separate publishing platform.

[10] *See, e.g.* Peter Swire, "The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations," OECD Conference (Virtual), (Mar. 27, 2020), https://peterswire.net/wp-content/uploads/PORT-IA.Swire_.March-27-2020.pdf (detailing a portability impact assessment to consistently evaluate the impact of portability initiatives across "competition, autonomy/user control, privacy, cybersecurity, and other legal or regulatory considerations").

Getting Data Portability Right

Our product development roadmap demonstrates one thing above all else: we want to build practical portability solutions people can trust and use effectively. To foster that trust, people and online services need clear direction about the objectives behind data portability obligations and the choices we make to build those solutions in a way that is both privacy-protective and consistent with those objectives.

There's growing agreement among policymakers around the world that data portability can help promote innovation online and encourage the emergence of new services.[11] Policy experts also agree that, although there are complicated issues involved, portability helps people control their data and can make it easier for them to choose among online service providers.[12]

Although some laws, such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Brazil's Lei Geral de Proteção de Dados (LGPD), already guarantee a right to portability, we believe companies and people would benefit from additional guidance about what it means to put those rules into practice.

Existing Portability Rights & Obligations

The principle of data portability is embodied in laws today. As mentioned, the GDPR, CCPA, and LGPD all include rights or obligations that allow for people to request that personal data or information be made available in a portable format or directly transmitted to another entity.[13] While broadly similar, the scope of data covered by each

---

[11] *See, e.g. A European Strategy for Data*, at 21, COM (2020) 66 final Feb. 2, 2020, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN; PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE, PUBLIC CONSULTATION ON REVIEW OF THE PERSONAL DATA PROTECTION ACT OF 2012 – PROPOSED DATA PORTABILITY AND DATA INNOVATION PROVISIONS 17 (May 22, 2019) [hereinafter PDPC PUBLIC CONSULTATION],

[12] *See, e.g.* Jason Furman et al., *Unlocking Digital Competition,* Report of the Digital Competition Expert Panel 9 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf ("There may be situations where opening up some of the data held by digital businesses and providing access on reasonable terms is the essential and justified step needed to unlock competition. Any remedy of this kind would need to protect personal privacy and consider carefully whether the benefits justified the impact on the business holding the data"); Stigler Comm. on Digital Platforms, STIGLER CTR. FOR THE STUDY OF THE ECONOMY & THE STATE, UNIV. OF CHICAGO BOOTH SCH. OF BUS., Final Report at 32 (2019), *available at* https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf; Eric Null & Ross Schulman, *The Data Portability Act: More User Control, More Competition*, OPEN TECHNOLOGY INSTITUTE (Aug. 19, 2019), https://www.newamerica.org/oti/blog/data-portability-act-more-user-control-more-competition/.

[13] *Compare* Regulation 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, 2016 O.J. L 119/1, art. 20

of these laws and the associated requirements on companies that must implement them do vary. As additional privacy regulations or dedicated portability laws come into effect, it is important for policymakers to keep in mind that consistency and harmonization of these regimes and the underlying intentions will help people and businesses alike.

Questions About Data Portability & Privacy

We think there are fundamental privacy questions that need to be answered for portability to be implemented successfully—meaning we can build privacy-protective, easy-to-use products for people at scale. As mentioned above, last year we published a white paper that sets forth five questions about data portability and privacy that we hope will help advance a global conversation about what it means to build privacy-protective data portability.[14] The full white paper is attached as an appendix to this submission.

After considering the challenges and proposals below, we urge the Commission to recommend dedicated federal portability legislation and provide advice to industry on these privacy questions, so that service providers implementing data portability have the clear rules and certainty necessary to build privacy-protective products that enhance people's choice and control online.

1. What is data portability?

Even though "data portability" is already written into laws in some places, the concept still means different things to different people. In our white paper we try to set out a taxonomy for distinguishing between different types of data transfers with the aim of identifying what is—and isn't—"data portability."

Based on some of the sources that discuss data portability, one might assume that it's a straightforward concept with a settled meaning. For example, the Article 29 Working Party explained that, in the GDPR context, portability is simply the right to receive personal data and transmit it from one service provider to another.[15] The International Organization for Standardization defines "data portability" as the "ability to easily transfer data from one system to another without being required to re-enter data," focusing on the ease with which data can be moved.[16]

[hereinafter GDPR], *with* CAL. CIV. CODE § 1798.100(d), *and* Lei No. 13.709 art. 18, de 14 de Agosto de 2018, D.O. de 15.08.2018. (Brazil).

[14] *Supra* note 3.

[15] *See* Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, at 5 (2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 [hereinafter Art. 29 Working Party, Guidelines].

[16] INTERNATIONAL ORGANIZATION FOR STANDARDISATION, ISO/IEC 19941:2017, Information Technology – Cloud Computing – Interoperability and Portability (2017), https://www.iso.org/obp/ui/#iso:std:66639:en.

In explorations of the literature on data portability and our conversations following over the last two years, we've found that there's considerable variation in people's views. In fact, we've heard calls—sometimes from the same stakeholder—both to enable greater data portability and to limit people's ability to share their data with third parties.[17]

Particularly following the Cambridge Analytica matter, we've consistently heard calls from various stakeholders to limit the information that users can share with apps through Facebook's consumer app platform ("Platform") and to enhance our oversight of the apps that do receive that information.[18] These calls suggest that some commentators may view the platform-to-app transfers of data as different from transfers made possible by "true" data portability. For example, Facebook's 2019 Consent Order with the FTC treats portability transfers separately from other transfers.[19]

It is important to recognize that most user-directed transfers of data to third parties look and operate similarly. But transfers that look similar technically may work differently in practice. One factor that differentiates transfers is the relationship between the transferring entity and the recipient entity and the rules, if any, that govern transfers between them. In general, these user-directed transfers of data to third parties can be thought of as occurring on a spectrum, with progressively more restrictions imposed as the relationship between the transferring entity and recipient entity grows closer.

At one end of the spectrum are *Open* transfers, user-directed transfers without controls or limitations (beyond those that exist under law) imposed on the recipient by the transferring entity. In the middle are *Conditioned* transfers, users can directly transfer

---

[17] *See* Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson, *In re Facebook, Inc.*, No. 0923184 (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf ([the Order] "requires greater oversight of third-party developers, including a requirement to terminate developers' access to users' information if they fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data"); and Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *United States v. Facebook, Inc.*, No. 19-cv-2184 (F.T.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf [hereinafter Facebook Decision and Order]. *But see* Separate Statement of Commissioner Noah Joshua Phillips, *Federal Trade Commission v. Unrollme Inc.*, No. 1723139 (Aug. 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1539865/phillips_-_unrollme_statement_8-8-19.pdf (suggesting that Google's restriction of third parties from using the information in the Gmail accounts of consumers for purposes such as market research or advertising, while promoted as a means to enhance consumer privacy, may also limit consumer choice and competition).

[18] *See, e.g.*, INFORMATION COMMISSIONER'S OFFICE, MONETARY PENALTY NOTICE (Oct. 24, 2018), https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, PIPEDA REPORT OF FINDINGS #2019-002 (Apr. 25, 2019), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/; Facebook Decision and Order *supra* note 17.

[19] Facebook Decision and Order *supra* note 17 at 3.

personal data to any recipient that has met certain conditions imposed by the transferring entity. The relationship between the transferring and recipient entities only exists for the purpose of enabling such user requests; there is no ongoing relationship. At the far end of the spectrum are *Partnership* transfers. Users can directly transfer personal data to a recipient with which the transferring entity has an ongoing relationship regarding such transfers, the terms of which may include provisions on how the recipient may use the data obtained in the transfer. Here, the relationship between the transferring and recipient entities exists for a purpose beyond simply effectuating users' transfer requests—such as, for example, integrating one of the entities' features into the other entity's products. Transfers through the Facebook Platform are an example of partnership transfers.

"This taxonomy (Open, Conditioned, Partnership) can be used to categorize data portability, other user-directed transfers of data, and even concepts like interoperability.[20] More significantly, it demonstrates how important it is to be intentional when designing data portability obligations and product implementations. Policymakers should keep in mind what objectives they are trying to achieve through regulation and how those regulations will shape products and user behavior in practice.

At a technical level, little distinguishes the APIs and data transfers that enable systems like Facebook's Platform and operating systems (like iOS and Android) from service-to-service portability tools like those enabled by the Data Transfer Project. It is the legal and policy frameworks (and their implicit aims) that surround application platforms and portability mechanisms that distinguishes them from each other, with significant impact on the privacy interests of people and the responsibilities of service providers.

As mentioned above, how people behave online figures heavily into our product decisions and should similarly inform regulatory and policy thinking.

[20] "Interoperability" is a concept that often figures into data portability conversations. It is complex and can mean different things in different contexts. Interoperability can mean the degree to which two systems/services have integrated implementations—like the ability of calls and data to transit two separate mobile networks. Interoperability can also mean the degree to which two systems can access data comparably and consistently—the ability of two different operating systems to render images in a JPEG format means that the format is interoperable. In the portability context, the former kind of interoperability might be a sort of user-directed *Partnership* transfer at the furthest end of the taxonomy we lay out. The latter kind of interoperability could describe how the Data Transfer Project relies on shared data models and import/export adapters to facilitate data portability between two different architectures. We observe that there may be challenges and costs to interoperability that should be carefully balanced against the anticipated benefits, including risks of homogenization of services and chilling innovation, as well as privacy, security, safety, and other challenges. How severe these risks and challenges may be would seem to depend in part on the nature and extent of the interoperability being discussed, making it important to clearly define "interoperability" when evaluating its merits and challenges.

For example, people often multihome in their use of online services[21] because of the simplicity of browsing to another site or downloading another app. Portability can further support that kind of consumer behavior. Data portability can assist people with the process of joining or trying a new app or service by enabling them to easily transfer profile information and data that would be relevant or useful to them in the new context. It should be noted that for online services that are part of, or bundled with, embedded operating systems (e.g. most mobile phones and personal computers), portability alone may not be as impactful as it can be for online services that are device independent. This is because having online services bundled with a device makes the cost of switching or multihoming higher, often including the price of a new device.

As the Commission evaluates whether and how data portability should be implemented in the U.S., we encourage them to consider the circumstances in which it would be most helpful to people. For Facebook, the principle of data portability is meant to give people control and choice while also fostering innovation. That informs how we design our products and is consistent with our view on how regulation should approach data portability obligations.

2. Which data should be portable?

In our white paper, we discuss different interpretations on what it means for a person to port the personal data they have "provided" to a service and the factors stakeholders should consider in defining the scope of portable data.

A primary purpose of enabling data portability is to provide individuals with control over their data. But what exactly is "their data"? It seems clear that people should be able to transfer "provided" data such as the photos they upload to a service or the posts they make to a social network. It's less clear what other data should be included.

Should people be able to export the information that a service provider receives as they use its features—information like search history, location data, and activity logs (often called "observed data")? What about information generated about people by the service provider on the basis of people's uploaded data or their interactions with the service, like the inferences (or "inferred data") used to personalize music, events, and ads, or to identify potentially fraudulent activity?

Another question—particularly when it comes to data about a person's use of a service—is how service providers' retention of data might bear on the question of which data should be portable. It seems uncontroversial that service providers should not be required to retain data solely for the purpose of enabling portability, so at least some data won't be portable simply because it won't be available at the time of the request. But what

[21] *See* Catherine E. Tucker, "Network Effects and Market Power: What Have We Learned in the Last Decade?" ANTITRUST 32, no. 2 at 76 (Spring 2018), *available at* http://sites.bu.edu/tpri/files/2018/07/tucker-network-effects-antitrust2018.pdf.

about the data that is technically available but will soon be deleted? Should a service provider build tools to export this data too?

Still another question is whether there are cases in which the burden of making data portable and understandable outweighs the person's interest in exporting it. For example, a service's data about a person's use of a service could include a list of every page or piece of content the person has viewed within a certain period, every link he or she has clicked on, and every notification he or she has received. Service providers often keep logs of this information for periods of time, but the process of making this log data portable could be challenging, and the benefits to the user might not always be obvious. These logs are not created for purposes of consumption outside the provider's bespoke systems; thus, making them portable may actually confuse and frustrate the requesting person.

Related challenges arise with non-human understandable data, such as outputs of machine learning systems, and data may be stored in formats that cannot be processed without access to proprietary technology—e.g., 3D data that requires underlying source code to render it. Should service providers be required to give recipients access to their proprietary systems to render ported data?

These examples also make clear that including all observed and inferred data could also result in a different sort of burden: the disclosure of trade secret or other proprietary information developed by a business to enhance or differentiate its services. Enabling people to port that kind of information could reduce incentives for businesses to develop it in the first place.[22]

Whether observed or inferred data should be included in a portability product can depend on a variety of factors, including privacy risks posed by a tool, the purpose behind it, and expectations of people. For example, Facebook has chosen to use DYI today to help to inform people about the data Facebook holds about them, and so inclusion of some observed and inferred data types makes sense given that purpose. Other tools, like our product based on the Data Transfer Project codebase, are meant to enable people to seamlessly move data between services. These tools involve transferring data to third parties over the Internet, which introduces different privacy and security risk (discussed further below). And so a scope of coverage for these tools that is narrower than the current scope of DYI could make more sense.

---

[22] *See* PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE, RESPONSE TO FEEDBACK ON THE PUBLIC CONSULTATION ON PROPOSED DATA PORTABILITY AND DATA INNOVATION PROVISIONS 5-7 (Jan. 20, 2020), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/Response-to-Feedback-for-3rd-Public-Consultation-on-Data-Portability-Innovation-200120.pdf?la=en (excepting confidential information and derived data from the scope of the proposed portability obligation "to encourage business innovation and ensure 'first movers' which bring to market innovative products/services are not prejudiced by the Data Portability Obligation and subject to unfair competition . . . ").

Since portability is partly intended to encourage innovation and the emergence of new services, we should consider these questions and competing interests in light of the costs to implement and maintain, the operational burden they would impose on service providers with fewer resources, and any chilling effect they would have on innovation. Viewed from that angle, it seems clear that some limitations should be imposed around a service provider's obligation to make observed and inferred data portable. Considering data retention periods and weighing the burden on providers against the benefit to users could be helpful in determining what those limitations should be or to whom they should apply.

Given the variability in the design and demands of portability tools, relative capacities of companies implementing portability requirements, impacts on innovation, and risks to the privacy of other people on the platform and the integrity of the service, our position is that portability obligations should not mandate the inclusion of observed and inferred data types.

3. Whose data should be portable?

Data is often associated with more than one person in digital services, like photos, videos and contact lists. Should transferring companies limit data portability in those cases? How can providers ensure that each individual's rights are accounted for?

Providing data portability helps people exercise control over their data. But what happens when one person wants to transfer data that is associated with another person?

- *Should I be able to take my friends' data to another service?*
- *What are my friends' rights to control their information in that scenario?*
- *What if people want to export the contents of their phone's address book or a list of their contacts' birthdays to a new service?*
- *Should a person's contacts—whose information would be shared with the new service—have a say in whether the person may share the information?*
- *Should I have the right to transfer a group photo uploaded by a friend if I'm in that photo?*
- *Should I have the right port content that I created jointly with other people, such as a shared photo album or a document where I drafted half the text?*

As these examples illustrate, it is sometimes difficult to delineate whose data should be transferred in response to a data portability request.[23] We've found this to be particularly

[23] *See, e.g.*, Dr. Aysem Diker Vanberg, *The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience*, 21(7) J. INTERNET L. 1, 3 (2018) ("[A]llowing one user to transfer a second user's information to another platform may violate the privacy rights of a second user."); Helena Ursic, *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, 15(1) SCRIPT-ED 42, 56 (2018), https://script-ed.org/wp-

true for Facebook, a core function of which is to allow users to connect with other people and create shared experiences. And the ability to transfer data about your contacts—or friends—can raise especially challenging privacy issues.[24] These issues grow more complex given the different ways that people can interact online and are further complicated by the introduction of concepts like data ownership, which we delve into further in our white paper.

Commentators often describe the question of whose data should be transferred in connection with portability as having to do with the portability of a person's "social graph"—the map of the connections between a user and other users and entities on that service. Some advocates of data portability have argued that services like ours must enable people to transfer their own data as well as data about their social graph, in part because the latter data may help enable other services to innovate.[25]

Without a portable social graph, these advocates argue, users may not be able to seamlessly transfer into alternative services. We think there are arguments on both sides: Enabling portability of the social graph can be important for innovation and user convenience, but doing so also comes with important privacy questions. The key question is whether we can find ways to enable this sharing that protects the privacy of all individuals involved.

---

content/uploads/2018/08/ursic.pdf (noting "additional difficulties in applying the right to data portability" when data contains "multiple persons' data which are . . . intertwined"); Barbara Engels, *Data Portability Among Online Platforms*, 5 INTERNET POL'Y REV., June 2016, 4-5, https://policyreview.info/articles/analysis/data-portability-among-online-platforms ("Allowing one to transfer a second user's information may violate the privacy rights of second user.").

[24] See Comments of New America's Open Technology Institute, *In re* Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition, at 4 (F.T.C. Aug 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf [hereinafter OTI Comments] ("[N]owhere is [the tension between the right to portability and friends' right of privacy] greater than when it comes to the portability of information about your contacts on social networks, or your 'social graph.'").

[25] *See* Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, ELECTRONIC FRONTIER FOUNDATION (July 24, 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine; Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, NEW AMERICA WEEKLY (June 28, 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends; *see also* Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, EUR. L. REV. 793, 804-05 (2017) ("[T]he inability to access ["friends" data] could constitute a barrier to entry for potential competitors."). *But see* Ben Thompson, *The Bill Gates Line Follow-up, Twitter and the Bill Gates Line, Data Portability and Facebook*, STRATECHERY (May 29, 2018), https://stratechery.com/2018/the-bill-gates-line-follow-up-twitter-and-the-bill-gates-line-data-portability-and-facebook/ (acknowledging that "forced data portability and interoperability" would "return[] Facebook to the state it was with the original social graph API," which is what prompted Cambridge Analytica).

Given the unresolved challenges of building portability products to account for these competing privacy interests, the initial version of our "Transfer a Copy of Your Photos and Videos" tool does not currently include information about friends tagged in photos or videos ported by users, nor are users able to transfer their friends' photos in which they are tagged. Feedback from stakeholders in conversations following publication of our white paper suggested that excluding social graph data is the best way to safeguard the privacy interests of non-requesting users and other third parties, until better technical and regulatory mechanisms are developed.

4. How should we protect privacy while enabling portability?

Although we're seeing proposed laws that require data transfers—including data portability laws—there is little guidance around protecting privacy in connection with those transfers. Stakeholders have raised concerns about the privacy and security risks of portability tools, and about the lack of clarity from policymakers and regulators about what is expected of transferring entities.[26]

More clarity on these points is key because in order for data portability to enhance people's control over their data, users should be able to trust that their data will be handled responsibly during and after the transfer. We've found it helpful to think through these questions about privacy and portability by considering transferring entities' actions with respect to (1) requesting users, (2) non-requesting users whose data would be transferred, and (3) recipient entities.

Requesting users

Communicating about privacy is challenging enough,[27] but communicating about privacy and data portability can be even more complex. Given that portability is about helping people stay in control of their data, it seems clear that transferring entities should focus on making sure that requesting users can make informed choices about transferring their

[26] *See, e.g.*, OTI Comments, *supra* note 24, at 4 ("Most services will now let you download your own social media posts, but what about other people's comments to those posts, or your comments and tags on other people's posts and photos? . . . . These are just some of the examples of the unresolved tension between my right to portability and my friends' right to privacy, and nowhere is that tension greater than when it comes to the portability of information about your contacts on social networks, or your 'social graph.'"); Lynskey, *supra* note 25, at 808 ("A further potential cost and complication for data controllers will be ensuring data security, given the tension between data security and data access. The A29WP perhaps underestimates the extent of this challenge for data controllers stating simply that the GDPR right may also 'raise some security issues' while highlighting that the data controller will remain responsible for 'taking all the security measures needed to ensure that personal data is securely transmitted[.]'"); Vanberg, *supra* note 23, at 7 ("The Article 29 Working Party arguably has not succeeded in offering more clarity as to what security standards are expected.").

[27] *See generally* Erin Egan, *Charting a Way Forward: Communicating About Privacy: Towards People-Centered and Accountable Design*, FACEBOOK (Jul. 14, 2020).

data. This means ensuring that requesting users have information about the entity to which they want their data to be transferred.

It can be difficult to strike a balance between giving people enough information to make an informed decision transferring their data to a third party but not so much that they are chilled from taking advantage of data portability tools entirely. But exactly what kind of information a person should have—and how it should be made available (and by whom)—are questions that haven't been fully answered by policymakers, regulators, or other stakeholders.

Non-requesting users

Some data portability requests may involve data associated with people other than the person making the portability request ("non-requesting users"). As discussed above, there are tough questions about whether these users' data should be transferred at all. If it should, service providers will need to account for the privacy interests of these users.

Some stakeholders have proposed consent mechanisms or similar means of allowing people to grant each other permission to have their data exported from a particular service—that is, for User A to be able to grant User B the permission to share User A's data with a recipient entity.[28] Given the focus on consent as part of a potential solution to the concern over the porting of non-requesting users' data, we want to explore whether—and, if so, how—services could offer meaningful choice and control to non-requesting users. Would requiring consent inappropriately restrict portability? If not, how could consent be obtained? Should, for example, non-requesting users have the ability to choose whether their data is exported each time one of their friends wants to share it with an app? Could an approach offering this level of granularity or frequency of notice could lead to notice fatigue?[29]

For users of a particular service, would it be better to give people a setting enabling them to always permit their friends (or other contacts) to transfer all—or certain categories—of their personal data to third parties? And how could we address non-users whose information is shared on a particular service?

---

[28] See Gennie Gebhart, Bennet Cyphers & Kurt Opsahl, *What We Mean When We Say "Data Portability,"* ELECTRONIC FRONTIER FOUNDATION (Sept. 13, 2018), https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability; Bankston, *supra* note 25.

[29] Notification fatigue is a problem often discussed in the breach notification context. *See, e.g.*, Jeri Clausing, *'Security Fatigue' Complicates the Battle Against Data Breaches*, INTERNET SOC'Y (Dec. 21, 2016), https://www.internetsociety.org/blog/2016/12/security-fatigue-complicates-the-battle-against-data-breaches/; *Christopher Mele, Data Breaches Keep Happening. So Why Don't You Do Something?*, N.Y. TIMES (Aug. 1, 2018), https://www.nytimes.com/2018/08/01/technology/data-breaches.html.

There has been considerable discussion, and some concrete proposals, about ways to enable the export of social graph information that implicitly offer some of the control and flexibility people desire without the drawbacks of some traditional mechanisms of notice and consent. Among these proposals, enabling the export of cryptographically obscured (or "hashed") versions of users' and their contacts' unique user identifiers has been described as "[p]erhaps the most promising avenue for social graph portability."[30] We explore these options in more detail in our white paper.

Potential recipients of personal data

As mentioned above, we've heard calls from many stakeholders that service providers should make additional efforts to protect against data misuse by at least certain third parties. But what should those efforts consist of when it comes to portability?

There is little expert commentary on this question. In the GDPR context, the Working Party's guidelines state only that a transferring data controller "is responsible for taking all the security measures needed to ensure . . . that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures)."[31] The guidelines suggest risk mitigation measures, such as using additional authentication information, or suspending or freezing transmission if there is suspicion that an account has been compromised. However, these security measures "must not be obstructive in nature and must not prevent users from exercising their rights[.]"[32]

Apart from these basic steps, the Working Party does not offer guidance on how service providers should protect against data misuse or other illicit or illegal behavior by third parties. Should service providers comply with user requests to port data to known bad actors or entities operating out of regions subject to sanctions? In conversations with stakeholders, we often hear that transferring service providers should consider imposing additional controls to ensure that recipients process user data with privacy and security in mind.

At the same time, we hear concerns that these kinds of requirements may be inconsistent with "true" portability: If people want to transfer their data to a particular entity, what business is it of the transferring entity to assess the purposes for which the person's data will be processed or whether the recipient complies with the law? What if the transferring entity and the recipient disagree about what the law requires? Should the transferring entity get to decide? There may be a point at which the transferring entity's efforts to exercise diligence beyond securing the transfer may impose undue friction on the abilities of users to try or switch to new or competing services.

---

[30] *See* OTI Comments, *supra* note 24, at 6-7.

[31] Art. 29 Working Party, *Guidelines*, *supra* note 15, at 19.

[32] *Id.*

As the portability ecosystem matures, it may be appropriate to partner on the complex questions raised by enabling data portability at scale with an independent mechanism or body that can reflect industry and other stakeholders' perspectives on data portability transfers and destinations. The independent mechanism could collaboratively set privacy and security standards to ensure data portability partnerships or participation in a portability ecosystem that are transparent and consistent with the broader goals of data portability.

One proposed response to such concerns is an accreditation system.[33] Under an accreditation model, potential recipients of user data could demonstrate, through certification to an independent body, that they meet the data protection and processing standards found in a particular regulation, such as the GDPR[34] or associated code of conduct. Accredited entities could then be identified with a seal and would be eligible to receive data from transferring service providers. The independent body (potentially in consultation with relevant regulators) could work to assess compliance of certifying entities, revoking accreditation where appropriate.

A key question for this model would be how to ensure that accreditation does not prove to be a barrier for small businesses and startups interested in taking advantage of portability. Another would be how it should treat recipient entities that fail to comply or choose not to certify. Even if a person's request to transfer information to such a recipient must be fulfilled, information about a recipient's noncompliance with (or refusal to sign on to) a scheme may still provide important information to users about the entity's privacy and security safeguards.

5. After people's data is transferred, who is responsible if the data is misused or otherwise improperly protected?

People and service providers need clarity on who is responsible for processing and protecting data before, during, and after a user-requested data transfer. Some have taken the position that platforms like Facebook may be responsible for ensuring that data

---

[33] *See* PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE, DISCUSSION PAPER ON DATA PORTABILITY 20 (Feb. 25, 2019), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf; Gus Rossi & Charlotte Slaiman, *Interoperability = Privacy + Competition*, PUBLIC KNOWLEDGE (Apr. 26, 2019), https://www.publicknowledge.org/news-blog/blogs/interoperability-privacy-competition ("[B]ecause they are dealing with personal data, third parties that want to interoperate would be required to follow a clear and transparent open model for user privacy, including potential requirements for pre-approval or certification by an independent entity."). *See also* Australian Government The Treasury, "Consumer Data Right Overview" (Sept. 2019), https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf (creating an accreditation system under which only entities that have been verified as meeting certain baseline privacy and information security requirements are permitted to be recipients of ported data).

[34] *See, e.g.*, GDPR, art. 42-43.

is protected following certain user-requested transfers of data to third parties.[35] This expectation, already challenging to implement in the immediate context of *Partnerships* transfers, becomes even more difficult to satisfy as data is transferred onward from recipients of those user-directed transfers. Should it be the expectation when it comes to data portability requests? And, if so, would such a rule chill the offering of portability solutions in the first place?

With respect to the exercise of the GDPR's portability right, the Working Party's guidelines provide a clear allocation of responsibility when a service provider ports data to another entity at a user's request.[36] Responsibility and liability generally follow user data to its new destination. Before and during any data transfer, the transferring service provider is responsible for ensuring that they act on the requesting user's behalf, securing the transmission on its way to the correct recipient, and mitigating any risks associated with data portability. Recipients must ensure that they receive only data that is necessary and relevant to the service they are providing to the requesting user.

After the transfer, the transferring service provider is not responsible for the processing handled by the data subject or by another company receiving personal data (since they are only acting on behalf of the data subject and not choosing the recipient organization). Instead, according to the Working Party, responsibility vests in the recipient, which must now process and protect the personal data it accepts according to its obligations under the GDPR.

This kind of an accountability framework seems to be most consistent with encouraging service providers to enable as much portability as possible. Other kinds of frameworks, like safe harbors in which liability protections inure only for transfers to accredited recipients, but not to unaccredited entities, might strike a balance between encouraging some portability while mitigating the risk of data misuse. The choices policymakers make in allocating responsibility when it comes to data portability will lead to differences in how portability tools and ecosystems develop, and the amount of choice and innovation portability may encourage.

Whatever the accountability framework, it is important that people and businesses have clearly established and consistent expectations of who is responsible for protecting data in portability contexts—before, during, and after the transfer. Clarity will foster trust in the ecosystem and allow people to vindicate their privacy interests should something go wrong.

Exploring the Frontiers of Data Portability

Following the publication of our white paper on data portability last year, and spurred by the development and launch of our recent portability tool, we've been having conversations with other stakeholders—companies, governments, academics,

[35] *See* sources cited *supra* note 18.
[36] *See* Art. 29 Working Party, *Guidelines*, *supra* note 15, at 6-7.

competition and data protection experts, startups, and consumer and privacy advocates—to figure out what the right framework is to enable portability that protects privacy and facilitates innovation and choice online. These conversations are informing our product development and have also led us to explore different models of data governance enabled by data portability.

Data Mobility Sandboxes

In addition to our participation in the Data Transfer Project, we've been working across industries to explore and expand upon questions around trustworthy data sharing and data portability from a cross-sectoral point-of-view.[37] How might future-facing data portability scenarios drive cross-sectoral service provision and ecosystem trust? There is still much to understand about how we make the portability ecosystem safe, easy, and valuable for people.

For example, there are various technical paradigms for accomplishing user-directed transfers. While our white paper and product work to date have focused on portability requests in which people bilaterally transfer data from one entity to another, researchers are currently developing multilateral models of portability that allow individuals to use intermediaries or data facilitators to manage their data from a variety of sources and decide where to store it and who may use it. For example, personal information management systems ("PIMS") let individuals store their data either locally or via cloud-based storage and let them "define at a sufficiently granular level how their personal information should be used and for what purposes."[38] In addition, an MIT project, "Solid," aims to create "decentralized social applications" that will allow individuals to move their information wherever they choose and switch between multiple platforms.[39]

That's why we're also participating in innovative projects like the Data Mobility Infrastructure Sandbox, which in 2019 explored the conditions for the safe porting of personal data through data facilitator models.[40] The next stage of this collaborative research project explored how multilateral, cross-sectoral data portability can generate value for people and businesses while mitigating risks and obstacles and accelerating potential market and service opportunities for people's wellbeing.

---

[37] *See* Datum Future, *Data Portability: What is at Stake?* (July 2019), https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf,

[38] *See* Eur. Data Protection Supervisor, EDPS Opinion on Personal Information Management Systems, Opinion 9/2016, at 7 (Oct. 20, 2016), https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_ en.pdf.

[39] *See* CSAIL-MIL, *What Does Solid Offer?*, solid, https://solid.mit.edu/.

[40] *See* Ctrl-Shift, *Release of Data Mobility Infrastructure Sandbox Report* (June 17, 2019), https://www.ctrl-shift.co.uk/news/2019/06/17/release-of-data-mobility-infrastructure-sandbox-report/.

Innovative approaches like these data mobility sandboxes bring together a variety of stakeholders in agile partnerships and help to quickly push the boundaries of existing policy and product thinking on data portability under the supervision of expert regulatory and non-governmental observers.

Conclusion

We are pleased to see the FTC devoting a full workshop to the benefits and complexities of data portability. We believe data portability can give people control and choice, while also fostering innovation.

We continue to invest in industry partnerships like the Data Transfer Project and building leading data portability products for our users based on feedback from the conversations that followed publication of our white paper on portability and privacy. In our experience, additional guidance as to the key policy and privacy questions we detail above would drive the development of the next generation of portability tools.

To that end, Facebook supports the passage of comprehensive federal privacy legislation in the United States, alongside dedicated portability legislation that can help guide the implementation of practical solutions. As policymakers and the Commission consider both privacy and portability regulation in the U.S., it is important to keep in mind that harmonization of these regimes with existing laws will help both people and businesses reap the benefits of data portability.

With respect to the outcomes of this workshop, we encourage the Commission to recommend dedicated federal portability legislation and provide advice to industry on the policy and regulatory challenges we raise in these comments, so that service providers implementing data portability have the clear rules and certainty necessary to build privacy-protective products that enhance people's choice and control online.

APPENDIX

SEPTEMBER 2019

CHARTING A WAY FORWARD

Data Portability and Privacy

Erin Egan

VICE PRESIDENT AND
CHIEF PRIVACY OFFICER, POLICY

FACEBOOK

Table of Contents

Data Portability and Privacy

01

There's growing agreement among policymakers around the world that data portability—the principle that you should be able to take the data you share with one service and move it to another—can help promote competition online and encourage the emergence of new services. Competition and data protection experts agree that, although there are complicated issues involved, portability helps people control their data and can make it easier for them to choose among online service providers.

The benefits of data portability to people and markets are clear, which is why our CEO, Mark Zuckerberg, recently called for laws that guarantee portability.[1] But to build portability tools people can trust and use effectively, we should develop clear rules about what kinds of data should be portable and who is responsible for protecting that data as it moves to different providers.[2] The purpose of this paper is to advance the conversation about what those rules should be.

We hope this paper will anchor a series of conversations among stakeholders around the globe about how to build portability products in a privacy-protective way while also helping keep competition vibrant among online services. At the conclusion of the series, we hope to have a portability framework that will improve our own and others' product development efforts, guide industry collaboration and potentially inform future legislation.

To that end, the paper sets out five questions about privacy and portability:

01 **What is "data portability"?**
Should all user-directed data transfers to third parties be considered "data portability"?

02 **Which data should be portable?**
Should portable data be limited to only the data a person has provided to the service provider (and what does it mean to "provide" data)?

03 **Whose data should be portable?**
If data is associated with more than one person—a common scenario for social networking services—should transferring providers limit data portability? How can providers ensure that each individual's rights are accounted for?

04 **How should we protect privacy while enabling portability?**
What responsibilities, if any, should transferring providers have with respect to (1) requesting users, (2) others whose interests may be implicated by a transfer, and (3) potential recipients of the data?

05 **After people's data is transferred, who is responsible if the data is misused or otherwise improperly protected?**
How should responsibility be allocated as between the transferring and recipient providers? Should users themselves be responsible for issues that affect their (or their friends') data?

We're fortunate to already have perspectives of key stakeholders on these questions, such as the EU data protection authorities' 2017 guidance on the right to data portability in the context of the European Union's General Data Protection Regulation ("GDPR"); two recent papers from Singapore's Personal Data Protection Commission; a report on competition policy in the digital era commissioned by the European Commission's Directorate-General for Competition; and a report on data mobility commissioned by the UK's Department for Digital, Culture, Media & Sport. But we believe the industry would benefit from additional discussion and guidance.

Importantly, this paper focuses on data portability as an action that individual users of a service choose to take; it does not focus on business-to-business transfers of information. We recognize that the latter transfers can be important to choice and competition, as well. That's why we're looking into ways to make data available to other companies that can, for example, help them train artificial intelligence models.

The privacy issues implicated by these kinds of transfers are different from those that arise when individuals choose to transfer their data. In this paper, we focus on transfers initiated by individuals, but we're continuing to engage with experts as we look into other types of transfers, as well.

Thank you in advance for participating in this crucial conversation. We welcome feedback from all stakeholders, and we look forward to hearing your thoughts.

The Challenge 02

One of our core privacy principles at Facebook is that we enable people to control the use of their information on our services.[3] Guided by that principle, we have built tools such as the controls that allow people to select the audience for their profile information and their posts, as well as Ad Preferences, which helps people control how their information is used to show them ads.

These tools help people control how their information is used on Facebook. But we also understand that giving people control means facilitating choice and competition by empowering them to move their information to a different service altogether—that we should, in other words, build products that enable data portability.

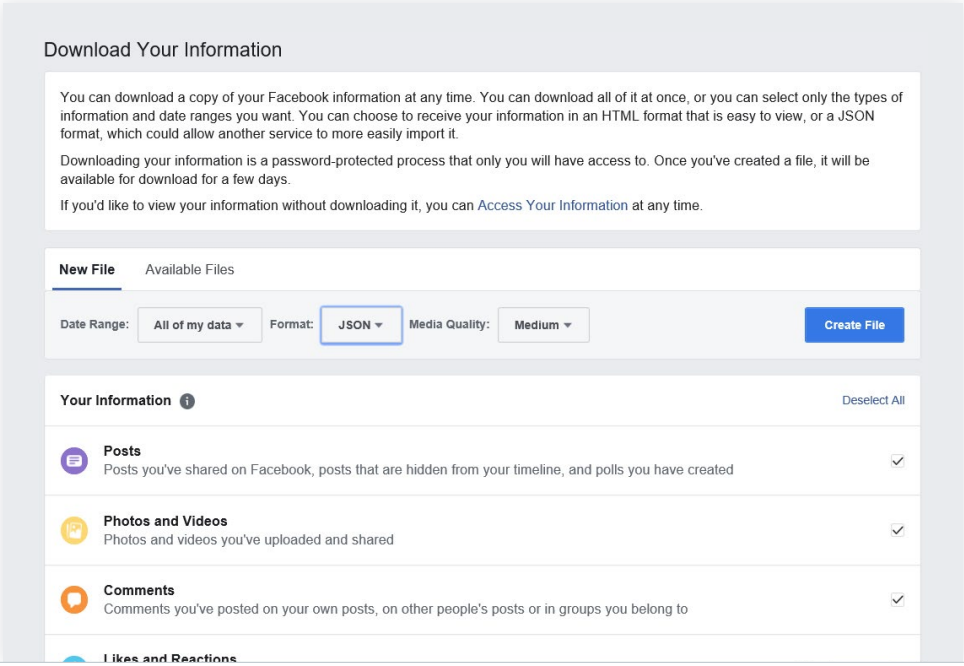
Data portability recently became a legal requirement in certain places through laws such as the GDPR[4] and the California Consumer Privacy Act ("CCPA"),[5] but Facebook has been considering ways to improve people's ability to transfer their Facebook data to other platforms and services for some time. For example, since 2010, we've offered Download Your Information ("DYI"), which is designed to help people access and share their information with other online services. In connection with the GDPR coming into force, we made DYI better suited for portability by enabling people to receive their information in the commonly used structured JSON format.

Although DYI is a robust data portability tool, we believe we can go further and improve choice and control by making it even easier for people to export their data to other services. In his recent op-ed, Mark Zuckerberg wrote that "[t]rue data portability should look more like the way people use our platform to sign into an app

than the existing ways you can download an archive of your information."[6] In other words, people should be able to transfer their information directly to a provider of their choosing, in a way similar to how people use Facebook Login today.

To help achieve this goal, we've joined Google, Microsoft, Twitter, Apple, and others in the Data Transfer Project, an open-source software project designed to help participants develop interoperable systems that allow individuals to transfer their data seamlessly between online service providers.[7] This project was inspired in part by the GDPR's right to portability, but we believe data portability will soon become the norm in other regions of the world. For example, California's new data portability provision will become effective in 2020; governments in Singapore, Australia, India, Hong Kong, and elsewhere may also soon pass laws supporting portability; and the European Commission is considering portability in the context of competition policy for the digital age.[8]

Proponents of portability recognize that, in order to succeed, industry needs to address potential fundamental privacy questions, such as those we pose in this paper.[9] But there has not been detailed guidance with respect to how service providers could or should balance the benefits to personal autonomy, innovation, and competition from portability against the potential risks to privacy and security.[10] For example, the EU's Article 29 Working Party (succeeded by the European Data Protection Board, which adopted its guidance) has recognized the risks to security posed by data portability tools—but has stated only that security measures should not "obstruct" people from exercising portability rights.[11] Similarly, the Working Party noted the importance of limiting a person's right to portability where its exercise could harm other people, but provided no specific guidance on how or when to implement this limitation.[12]



In addition, some guidance on portability seems at odds with other guidance on companies' responsibilities for protecting against data misuse by third parties to which companies enable data transfers. Privacy regulators have made it clear that, at least in the context of some third-party relationships, platforms like ours should have protections in place that account for the privacy risks that can arise from transfers.[13] But with respect to the GDPR's right to portability, the Working Party both endorses the idea of enabling people to disclose their data to third parties[14] and states that "the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient."[15]

Several reports on competition in digital markets have emphasized the value of portability for innovation, and have noted that we need to address potential privacy and security risks. For instance, the report of the UK's Digital Competition Expert Panel stated that "[a]ny approach to support this form of data sharing will also have to ensure that robust privacy safeguards are adopted to respect the privacy rights and expectations of users."[16] But the report does not expand on what those safeguards should be.

As we move toward a world of greater portability, we and other companies would benefit from clear rules that help resolve these kinds of questions—questions about portability, privacy and responsibility.

Five Questions About Portability and Responsibility

03

As discussed above, data portability helps people control their data and choose the services that best meet their needs. At the same time, portability can present challenges to safeguarding privacy interests. To address these challenges, we're seeking feedback and guidance from a wide range of stakeholders about how to build portability in a way that empowers people and fosters competition while maintaining their trust in online services.[17] In this section, we set out five key questions, the answers to which will help build the next generation of portability products. We also offer some thoughts on how to answer these questions to help further the conversation on these important topics.

QUESTION 1

What is "Data Portability"?

Based on some of the sources that discuss data portability, one might assume that it's a straightforward concept with a settled meaning. For example, the Article 29 Working Party explained that, in the GDPR context, portability is simply the right to receive personal data and transmit it from one service provider to another.[18] The International Organization for Standardization defines "data portability" as the "ability to easily transfer data from one system to another without being required to re-enter data," focusing on the ease with which data can be moved.[19]

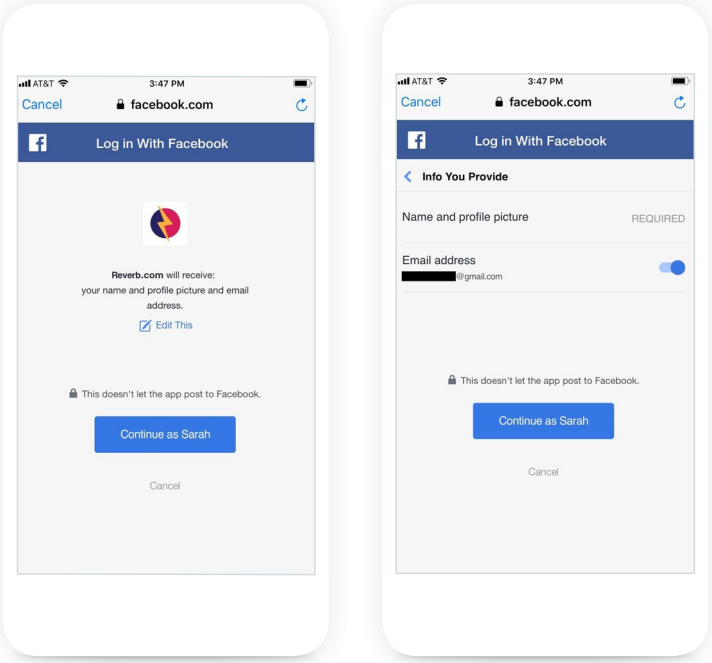
But when we move beyond esoteric discussions of portability, we find that there's considerable variation in people's views. In fact, we've heard calls—sometimes from the same stakeholder—both to enable greater data portability and to limit people's

ability to share their data with third parties.[20] The context in which we typically hear the latter is in connection with our consumer app platform (or "Platform" for short), which, among other things, refers to the set of technologies we make available for developers that want to enable people to (1) share their Facebook information with the developer's app or (2) send information from the developer's app to Facebook. The best-known Platform tool is Facebook Login, which enables people to log in to—and share their information with—third-party apps.

Particularly following the Cambridge Analytica matter, we've consistently heard calls from various stakeholders to limit the information that apps can receive through Facebook Login and to enhance our oversight of the apps that do receive that information.[21] These calls suggest that some commentators may view the platform-to-app transfers of data as different from transfers made possible by "true" data portability. For example, Facebook's 2019 Consent Order with the FTC treats portability transfers separately from other transfers.[22]

By contrast, other commentators have suggested that Cambridge Analytica happened because of data portability, implying that platforms like ours (as well as iOS, Android, Twitter, and others) were already engaging in data portability when we enabled people to share their data with apps on Platform.[23]

The question that comes out of these conversations is: When is a person's request to transfer data a *portability* request? The answer is crucial, not least because of the legal rights that attach to portability requests. Under the GDPR, for example, portability requests must be fulfilled "without hindrance," raising questions about whether there are any circumstances in which a service provider may deny a request, limit the data available in response to the request, or restrict the third party's ability to use the data following the transfer. It's clear that many stakeholders believe platforms should impose data-use restrictions on recipients of user data, but the question remains whether service providers must make alternative mechanisms available to enable transfers without such restrictions. If so, how are these two transfers different from each other?



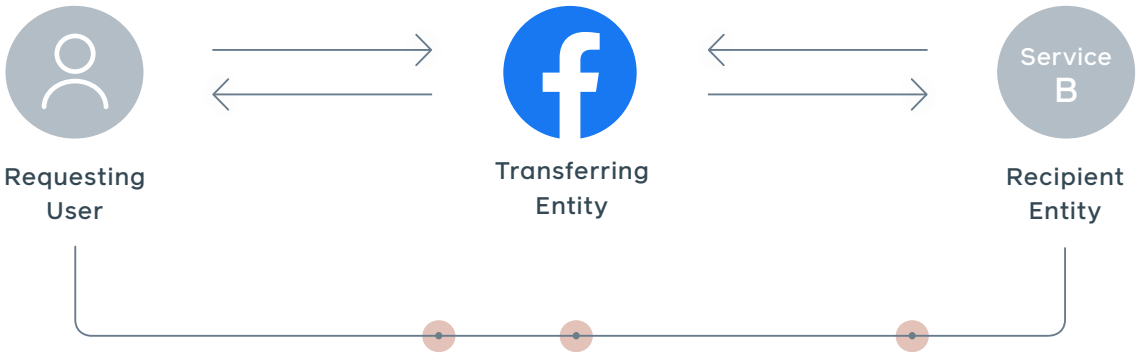
To begin to answer this question, it is important to recognize that most user-directed transfers of data to third parties look and operate similarly. Transfers generally involve three parties: requesting users, transferring entities, and recipient entities.[24]

From a technical perspective, a data transfer begins when the requesting person instructs the transferring entity to export his or her data. The transferring entity then sends the requested data either to the requesting person (who then may use the data or send it to the recipient entity) or directly to the recipient entity. Once the data is shared with the recipient entity, the user can then interact with the data on or through that service.

But transfers that look similar technically may work differently in practice. One factor that differentiates transfers is the relationship between the transferring entity and the recipient entity and the rules, if any, that govern transfers between them. In general, these user-directed transfers of data to third parties can be thought of as occurring on a spectrum, with progressively more restrictions imposed as the relationship between the transferring entity and recipient entity grows closer (setting aside, for the moment, what the scope of the data transferred should be, which we discuss later in the paper). Three broad categories of user-directed transfers could be described as follows:

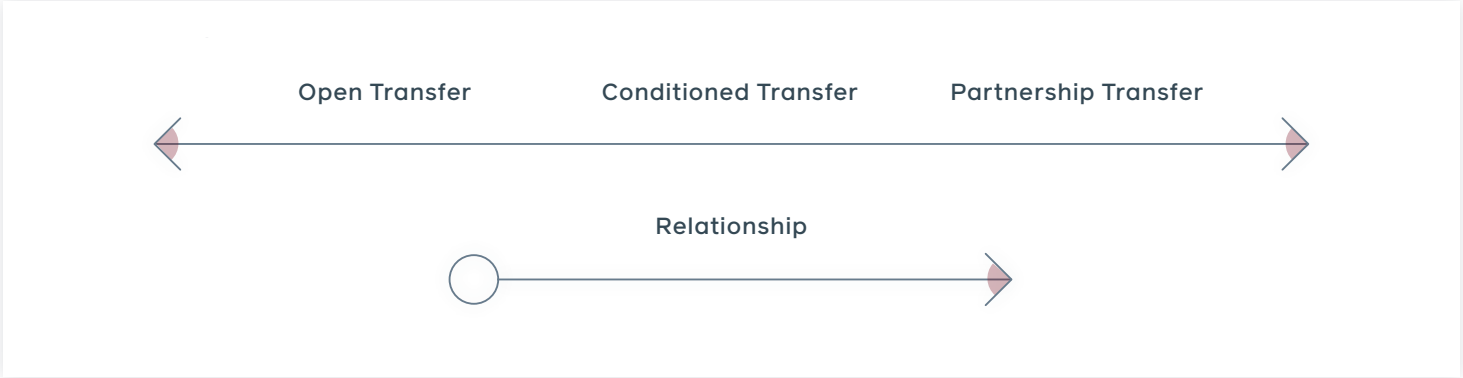
1. OPEN TRANSFERS

Requesting users can receive their data and transfer it to any recipient entity without controls or limitations (beyond those that exist under law) imposed on the recipient by the transferring entity. In this model, either the users can perform the transfer to a recipient via their own device (as in our DYI tool) or the transferring entity can facilitate a direct transfer. Apart from the technical connection made for the purpose of enabling a transfer, there is no relationship between the transferring and recipient entities. This model seems closest to that anticipated by the GDPR and the Working Party guidance.



2. CONDITIONED TRANSFERS

Requesting users can receive their data and transfer it to any recipient that has met certain conditions imposed by the transferor. The relationship between the transferring and recipient entities only exists for the purpose of enabling such user requests; there is no ongoing relationship. As we examine below, this could be a way to think about user requests to port data directly between services, the technical means for which the Data Transfer Project is working toward.



3. PARTNERSHIP TRANSFERS

Requesting users can receive their data and transfer it to a recipient with which the transferor has an ongoing relationship regarding such transfers, the terms of which may include provisions on how the recipient may use the data obtained in the transfer. Here, the relationship between the transferring and recipient entities exists for a purpose beyond simply effectuating users' transfer requests—such as, for example, integrating one of the entities' features into the other entity's products. Transfers through the Facebook Platform are an example of partnership transfers.

When thinking about portability, it helps to acknowledge the differences between these categories of user-directed data transfers. The question we need to answer is which transfers should be considered as involving "data portability" and what obligations on each party in the transaction, if any, should flow from each model? Open transfers seem to be clearly consistent with the nature of data portability as described in the GDPR and elsewhere, but what about conditioned transfers, in which the transferring entity may choose to limit the third parties to which the user may send data? Are such limitations consistent with the right to portability? Should partnership transfers—like the transfers from Platform—ever be viewed as involving data portability?

In our conversations with stakeholders so far, the general view about these questions has been that a transferring entity may—and should—impose some

baseline privacy and data protection restrictions around transfers even when carrying out the transfer to comply with a portability request. But, as discussed below, questions remain about what kinds of conditions are appropriate. Restrictions along the lines of those we impose through Platform strike some as too restrictive to be consistent with portability. Our recent settlement with the FTC suggests that some regulators may view Platform-style transfers as distinct from portability transfers.[25] Where the line is between these two categories will likely be the line between portability and other data transfers.

QUESTION 2

Which Data Should be Portable?

A primary purpose of enabling data portability is to provide individuals with control over their data. But what exactly is "their data"? It seems clear that people should be able to transfer data such as the photos they upload to a service or the posts they make to a social network. It's less clear what other data should be included.

Should people be able to export the information that a service provider receives as they use its features—information like search history, location data, and activity logs? What about information generated about people by the service provider on the basis of people's uploaded data or their interactions with the service, like the inferences used to personalize music, events, and ads, or to identify potentially fraudulent activity?

The GDPR and the Working Party guidance suggest that there should be limits around the data that is subject to the portability right. The GDPR requires portability of personal data that a person has "provided to" a data controller.[26] The Working Party has suggested that people be able to transfer personal data that they **actively provide** to a service provider or that the service provider **observes** about them as they use its services, but not data that the service provider **infers** about them based on that use.[27]

Another question—particularly when it comes to data about a person's use of a service—is how service providers' retention of data might bear on the question of which data should be portable. It seems uncontroversial that service providers should not be required to retain data solely for the purpose of enabling portability, so at least some data won't be portable simply because it won't be available at the time of the request. But what about the data that is technically available but will soon be deleted? Should a service provider build tools to export this data too?

Still another question is whether there are cases in which the burden of making data portable outweighs the person's interest in exporting it. For example, a service's data about a person's use of a service could include a list of every page

or piece of content the person has viewed within a certain period, every link he or she has clicked on, and every notification he or she has received. Service providers often keep logs of this information for periods of time, but the process of making this log data portable could be challenging, and the benefits to the user might not always be obvious. Would it be useful, for example, to be able to export a list of all the links you've clicked on Facebook within a certain period? Or an archive of every ad you've seen while scrolling through News Feed?

Given that portability is partly intended to encourage competition and the emergence of new services, we should consider these questions in light of the operational burden they would impose on service providers with fewer resources than companies like Facebook. Viewed from that angle, it seems clear that some limitations should be imposed around a service provider's obligation to make observed data portable. Considering data retention periods and weighing the burden on providers against the benefit to users could be helpful in determining what those limitations should be or to whom they should apply.[28] But we will need to answer questions about how any balancing should be conducted—and by whom.

QUESTION 3

Whose Data Should be Portable?

Providing data portability helps people exercise control over their data. But what happens when one person wants to transfer data that is associated with another person? What if, for example, Person A wants to move her photos from one service to another, but those photos include images of Person B? What are Person B's rights to control his information in that scenario? What if people want to export the contents of their phone's address book or a list of their contacts' birthdays to a new service? Should a person's contacts—whose information would be shared with the new service—have a say in whether the person may share the information?

As these examples illustrate, it is sometimes difficult to delineate whose data should be transferred in response to a data portability request.[29] We've found this to be particularly true for Facebook, a core function of which is to allow users to connect with other people and create shared experiences. And the ability to transfer data about your contacts—or friends—can raise especially challenging privacy issues.[30]

Some have suggested that the only data that should be transferred following a portability request should be the data that the requesting person "owns."[31] If the requesting users own the data they provide to a service, the argument goes, then they should be able to do whatever they wish with it, including porting it to another entity. Conversely, if requesting users do not own some of the data they wish to transfer, then they should not be able to port that data.

The concept of data as property has been viewed by some as controversial and may lead to *more* questions that stretch well beyond the portability context.[32] For example, in practice, many types of information have more than one owner. If you have my phone number in your address book, for example, are you the owner of that phone number? Moreover, in the EU, data protection (as a fundamental right) does not vary depending on who, if anyone, "owns" the data in question.[33]

Another approach to deciding whose data should be made portable in response to a request could be based on factors such as who provided the data, whether the service provider has associated it with a particular user, and the sensitivity of the data. Consider the following scenario:

Person A uploads a video of herself and three of her friends (Persons B, C, and D). She doesn't take any steps that would enable the service to identify her friends (such as "tagging" them). At first glance, it seems clear that Person A should have the right to port the video to a new service, but what rights, if any, should Persons B, C, and D have with respect to the video? And who is best positioned (as between Person A and the service provider) to address those rights?

Now consider a slightly different version of the same scenario: Person A uploads the video,but this time, she tags Persons B, C, and D, who all happen to be users of the service. In this scenario, the service provider may be in a position to inform Persons B, C, and D about a portability request. Assuming this happens, should they have the right to stop Person A from transferring the video?

How might the answers change if, instead of a video, we were talking about email addresses in Person A's contacts list? Should it be easier or harder for Person A to port them than to port Person A's photos? What about emails themselves, which a person might want to export to a new email service (e.g., from Gmail to Outlook)?

We think a multifactor approach that considers questions like these and the factors above is likely preferable to an approach that focuses on data ownership. But *how we weigh these factors* in the analysis of whose data should be portable requires much more discussion and guidance.[34]

Commentators often describe the question of whose data should be transferred in connection with portability as having to do with the portability of a person's "social graph"—the map of the connections between a user and other users and entities on that service. Some advocates of data portability have argued that services like ours must enable people to transfer their own data as well as data about their social

graph, in part because the latter data may help enable other social networking companies to innovate.[35] Without a portable social graph, these advocates argue, users may not be able to seamlessly transfer into alternative social networks.

We think there are strong arguments on both sides: Enabling portability of the social graph can be important for innovation and competition, but doing so also comes with important privacy questions. The key question is whether we can find ways to enable this sharing that protect the privacy of all individuals involved. We turn to this issue in the next section.

QUESTION 4

How Should We Protect Privacy While Enabling Portability?

Questions 1 through 3 involve questions about circumstances before people choose to port their data. Once we know (1) that we're dealing with a user-directed transfer of data, (2) which types of data should be transferred, and (3) whose data should be transferred, we next need to ask how we can enable portability while protecting privacy.

Although we're seeing laws that require data transfers—including data portability laws—there is little guidance around protecting privacy in connection with those transfers. Stakeholders have raised concerns about the privacy and security risks of portability tools, and about the lack of clarity from policymakers and regulators about what is expected of transferring entities.[36]

More clarity on these points is key because in order for data portability to enhance people's control over their data, users should be able to trust that their data will be handled responsibly during and after the transfer. We've found it helpful to think through these questions about privacy and portability by considering transferring entities' actions with respect to (1) requesting users, (2) non-requesting users whose data would be transferred, and (3) recipient entities.

REQUESTING USERS

Given that portability is about helping people stay in control of their data, it seems clear that transferring entities should focus on making sure that requesting users can make informed choices about transferring their data. This means ensuring that requesting users have information about the entity to which they want their data to be transferred. But exactly what kind of information a person should have—and how it should be made available (and by whom)—are questions that haven't been fully answered by policymakers, regulators, or other stakeholders.

In its assessment of portability under the GDPR, the Working Party explained that although people are "responsible" for "identifying the right measures in order to secure personal data" with the entity to which they'll transfer their data, the transferring entity should make the data subject "aware" of measures to enable the person to take appropriate steps.[37]

Compare that guidance with a recent discussion paper from Singapore's Personal Data Protection Commission, which suggests that transferring entities should go further, including by providing information such as how user data will be used by the data recipient; the nature of the new product or service that the user is acquiring; and the track record, reputation, and data management and protection practices of the data recipient.[38] In its May 2019 consultation paper on the topic, the Commission further proposed requiring organizations to provide relevant information to people as part of a binding code of practice.[39]

These perspectives are helpful starting points, but we think there's more to discuss about what, if any, information should be provided to people who want to transfer their data—as well as how, and by whom, that information could be presented in a helpful way.

NON-REQUESTING USERS

Some data portability requests may involve data associated with people other than the person making the portability request ("non-requesting users"). As discussed above, there are tough questions about whether these users' data should be transferred at all. If it should, service providers will need to account for the privacy interests of these users.

Some stakeholders have proposed consent mechanisms or similar means of allowing people to grant each other permission to have their data exported from a particular service—that is, for User A to be able to grant User B the permission to share User A's data with a recipient entity.[40] Given the focus on consent as part of a potential solution to the concern over the porting of non-requesting users' data, we want to explore whether—and, if so, how—services could offer meaningful choice and control to non-requesting users. Would requiring consent inappropriately restrict portability? If not, how could consent be obtained? Should, for example, non-requesting users have the ability to choose whether their data is exported each time one of their friends wants to share it with an app? Would such an approach lead to notice fatigue?[41] For users of a particular service, would it be better to give people a setting enabling them to always permit their friends (or other contacts) to transfer all—or certain categories—of their personal data to third parties? And how could we address non-users whose information is shared on a particular service?

A. Portablility of Social Graph Data

As discussed above, some stakeholders view the transfer of social graph information (such as contacts lists) as an important way to help emerging social networking companies innovate and develop new services.[42] There has been considerable discussion, and some concrete proposals, about ways to enable the export of this kind of information. Among these proposals, enabling the export of cryptographically obscured (or "hashed") versions of users' and their contacts' unique user identifiers has been described as "[p]erhaps the most promising avenue for social graph portability."[43]

This solution aims to hide user IDs (e.g., email addresses) from the recipient entity while still providing some ability to reconstruct the transferring users' social graph, potentially helping address the privacy challenges of sharing friends' data with third parties by avoiding unnecessary exposure of personal data. However, experts have noted that this proposal would "require a major collaborative technical effort that could raise unanticipated privacy and security challenges as well as legal compliance questions[.]"[44] Below, we explore two commonly discussed approaches to sharing hashed contacts' data and the potential challenges such approaches could raise.

First, a provider could share a list of hashed identifiers that are associated with the requesting user and their contacts. The simplest way of doing this is to share hashed versions of a contact's name (which is not necessarily unique) or email address. If Users A and B are both connected to User C, and both share their hashed contacts' lists with a service, then that service will know that User A and User B are both connected to User C, but it cannot learn additional information about User C unless User C has also ported his or her personal data to the same service.

Another option is to share identifiers not associated with users but rather with relationships between users. In this system, if Users A and B are both friends with User C, and both share their contacts lists, then—unlike above—the recipient service cannot know that Users A and B are both friends with User C. This is because the identifier for the relationship between Users A and C is different from the identifier for the relationship between Users B and C. However, if User C chooses to also share their contacts list, then User C will share the same two identifiers for their relationship with Users A and B respectively, at which point the receiving service can match up these identifiers to know that User C is connected to User A and User B.

Both of these approaches have drawbacks that require further discussion with stakeholders. In the first approach, it may be possible for the recipient to infer information about User C based solely on their relationship with Users A and B. For example, if Users A and B share an employer or are members of the same political party, then the recipient may be able to infer those facts about User C and

determine User C's identity with minimal additional information. The second approach doesn't suffer from this issue, but its utility to the recipient may be more limited because a relationship is only recognizable by the recipient service if both contacts choose to share their information with the recipient service.

Another challenge for social graph sharing is to settle upon a common data model that is specific enough to be useful but broad enough to apply across services. For example, some social networks have a single account per user, while others allow multiple accounts for one user. If User A is connected with one of User B's accounts but not with another, how should this relationship be reflected when either user shares a contacts list with a service that permits only a single account per user? Further risk of data leakage is introduced when users who port contacts data from a pseudonymous social network to one that requires real names. Recipients (or even the requesting user) may be able to infer the actual identities of pseudonymous users based on commonalities with their known contacts.

Moreover, social graph sharing can grow more complex as we consider additional layers of social interaction. For example, if one of User A's posts is ported to another social network and User B has commented on or liked that post, when should that comment be visible, who should be able to see it, and how should User B be identified, if at all, on the new service? The answers to those questions could vary based not only on the audience controls at the new service, but also on the mechanism used to port and identify contacts at the new service.

POTENTIAL RECIPIENTS OF PERSONAL DATA

Over the past year, we have heard calls from many stakeholders that service providers should make additional efforts to protect against data misuse by at least certain third parties.[45] But what should those efforts consist of when it comes to portability?

There is little expert commentary on this question. In the GDPR context, the Working Party's guidelines state only that a transferring data controller "is responsible for taking all the security measures needed to ensure . . . that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures)."[46] The guidelines suggest risk mitigation measures, such as using additional authentication information, or suspending or freezing transmission if there is suspicion that an account has been compromised. However, these security measures "must not be obstructive in nature and must not prevent users from exercising their rights[.]"[47]

Apart from these basic steps, the Working Party does not offer guidance on how service providers should protect against misuse by third parties. In conversations with stakeholders, we often hear that transferring service providers should consider

imposing additional controls to ensure that recipients process user data with privacy and security in mind. For instance, providers could require recipients to certify (1) the purposes and uses for the personal data they may receive pursuant to a data portability request, and (2) that they are processing data in accordance with applicable laws and data protection requirements. We also hear that providers should even consider monitoring recipient entities' processing of data and enforcing against recipient organizations who fail to process data according to applicable laws and data protection requirements, an extremely challenging (if not impossible) requirement and one that seems not to be required under the GDPR formulation of portability.

At the same time, we hear concerns that these kinds of requirements may be inconsistent with "true" portability: If people want to transfer their data to a particular entity, what business is it of the transferring entity to assess the purposes for which the person's data will be processed or whether the recipient complies with the law? What if the transferring entity and the recipient disagree about what the law requires? Should the transferring entity get to decide? There may be a point at which the transferring entity's efforts to exercise diligence beyond securing the transfer may impose undue friction on the abilities of users to switch to competing services.

One proposed response to such concerns is an accreditation system.[48] Under an accreditation model, potential recipients of user data could demonstrate, through certification to an independent body, that they meet the data protection and processing standards found in a particular regulation, such as the GDPR.[49] Accredited entities could then be identified with a seal and would be eligible to receive data from transferring service providers. The independent body (potentially in consultation with relevant regulators) could work to assess compliance of certifying entities, revoking accreditation where appropriate.

Another potential solution, which may be compelling to providers that operate in a country without a comprehensive data protection framework, could be the creation of a portability-focused code of conduct administered by an independent organization.[50] The code of conduct could require entities to implement privacy and security safeguards before receiving user-requested data. The independent organization could engage in monitoring and enforcement of its signatories for potential violations. A key question for this model would be how it should treat recipient entities that fail to comply with or don't sign on to the code. Even if the user's request to transfer information to such a recipient must be fulfilled, information about a recipient's noncompliance with (or refusal to sign on to) the code of conduct may still provide important information to users about the entity's privacy and security safeguards.

QUESTION 5

After people's data is transferred, who is responsible if the data is misused or otherwise improperly protected?

People and service providers need clarity on who is responsible for processing and protecting data before, during, and after a user-requested data transfer. Regulators have taken the position that platforms like Facebook may be responsible for ensuring that data is protected following certain user-requested transfers of data to third parties. Is that the case when it comes to data portability requests?

With respect to the exercise of the GDPR's portability right, the Working Party's guidelines provide a clear allocation of responsibility when a service provider ports data to another entity at a user's request.[51] Responsibility and liability generally follow user data to its new destination. Before and during any data transfer, the transferring service provider is responsible for ensuring that they act on the requesting user's behalf, securing the transmission on its way to the correct recipient, and mitigating any risks associated with data portability. Recipients must ensure that they receive only data that is necessary and relevant to the service they are providing to the requesting user.

After the transfer, the transferring service provider is not responsible for the processing handled by the data subject or by another company receiving personal data (since they are only acting on behalf of the data subject and not choosing the recipient organization). Instead, according to the Working Party, responsibility vests in the recipient, which must now process and protect the personal data it accepts according to its obligations under the GDPR.

The Personal Data Protection Commission of Singapore's discussion paper also proposes a liability model, in which transferring entities would be exempted from claims for damage arising from misuse of data by the recipient—a result the Commission believes appropriate, given that transferors cannot feasibly vet all potential recipients. The paper also states that the transferor should not be liable for claims "relating to the accuracy and quality of the ported data unless it was demonstrated that the data was corrupted while under the care of the [transferor]."[52] In its most recent consultation paper on the topic, the Commission does not mention liability but appears to limit post-transfer responsibilities for transferor entities to "check[ing] that the data transmitted has been received by the receiving organization and assist[ing] with any queries it may have with respect to the data transmitted."[53]

But there are clearly some circumstances in which policymakers and regulators expect transferring entities to maintain responsibility even after the transfer. One

way to harmonize this reality with the Working Party's guidelines and the Personal Data Protection Commission's discussion paper may be to further clarify that service provider responsibility may vary depending on where on the spectrum a transfer falls—i.e., whether it is an open transfer, a conditioned transfer, or a partnership transfer, as discussed in Section II.A. For instance, should providers be deemed more accountable in a partnership transfer (e.g., a model like Facebook's Platform) due to the closer nature of their relationship with the recipient organization and a purpose for the transfer that extends beyond satisfying a request from a user?

For open transfers, perhaps the most a service provider should be responsible for is helping users take responsibility for the risks associated with taking their data to a new service; provided this has occurred, responsibility for protecting data would rest solely with the recipient. Service providers might explore tools to help users understand security risks and protocols for their downloaded data. Providers could also consider giving users guidance on how to inspect recipient organizations for potential abuse or insufficient security safeguards. For instance, providers could teach users ways to confirm the authenticity of the recipient organization (that it is what it says it is); check the website security for recipient organizations (e.g., the difference between HTTP and HTTPS); secure their devices when they download data (e.g., not using public Wi-Fi when downloading data); and identify whether the recipient organization has appropriate policies in place (e.g., checking privacy policies to determine whether an entity will sell user data that it receives).

For conditioned transfers, one approach would be for service providers to require recipients to certify that they're accredited by a standards body, in compliance with a relevant code of conduct, or otherwise that they will process personal data in accordance with applicable laws and data protection requirements before fulfilling a transfer request. Once providers have received such a certification, they could be relieved of responsibility (and liability) for data issues that arise after transfer.

For partnership transfers, it may be more appropriate to impose some degree of responsibility on the transferring entity, even for conduct that occurs after the transfer. To the extent feasible, some enhanced oversight of recipients' handling of people's data following a transfer may also be appropriate.

Finally, there is the complex question of responsibility when it comes to individuals about whom data is transferred by another party as part of a portability request. The Working Party guidelines note that if a user's data portability request involves personal data belonging to third parties, the requesting user is also responsible for the processing operations that the user initiated (to the extent that such processing is not decided by the controller), outside of an exemption for household or personal use.[54] Imposing responsibility (and liability) for requesting users who transfer contacts' data could chill interest in portability generally, and in social graph

portability specifically. Could a better outcome be to limit liability for requesting users to only cases involving truly unreasonable or reckless behavior, such as knowingly transferring their contacts' data to a party known to have a history of data misuse or poor data protection practices?

What's Next? 04

Data portability promises to give people unprecedented control of their information and to support continued vibrant innovation and competition online. The GDPR and other laws have prompted considerable investment in portability tools. This paper and the conversations that will follow it are intended to promote portability by laying out the issues and starting to address hard questions about how portability can be implemented in a privacy-protective way. We strongly believe that it can, and we look forward to collaborating with a range of stakeholders on solutions in the months to come.

Data Portability and Privacy: Charting a Way Forward

1. *See* Mark Zuckerberg, *The Internet Needs New Rules. Let's Start in These Four Areas,* Wash. Post (March 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.6247ef86cd32.
2. *See id.*
3. *Facebook Privacy Principles,* Facebook, https://www.facebook.com/about/basics/privacy-principles (last visited Aug. 16, 2019).
4. Regulation 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, 2016 O.J. L 119/1, art. 20 [hereinafter GDPR].
5. Cal. Civ. Code § 1798.100(d) (effective Jan. 1, 2020).
6. Zuckerberg, *supra* note 1.
7. *See About Us,* Data Transfer Project, https://datatransferproject.dev/ (last visited Aug. 16, 2019).
8. *See* Jacques Crémer, et al., *Competition Policy for the Digital Era*, Report for the European Commission (2019), http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.
9. *See* Jason Furman et al., *Unlocking Digital Competition*, Report of the Digital Competition Expert Panel 9 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf ("There may be situations where opening up some of the data held by digital businesses and providing access on reasonable terms is the essential and justified step needed to unlock competition. Any remedy of this kind would need to protect personal privacy and consider carefully whether the benefits justified the impact on the business holding the data").
10. *See, e.g.*, *Datum Future*, *Data Portability: What is at stake?* (July 2019), https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf.
11. *See* Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, at 19 (2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 [hereinafter Art. 29 Working Party, Guidelines].
12. *Id.* at 11.
13. *See, e.g.*, Information Commissioner's Office, Monetary Penalty Notice (Oct. 24, 2018), https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf; Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2019-002 (Apr. 25, 2019), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/; Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *United States v. Facebook, Inc.*, No. 19-cv-2184 (F.T.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf [hereinafter Facebook Decision and Order].
14. *See* Art. 29 Working Party, *Guidelines, supra note* 11, at 19.
15. *See id.* at 6 (emphasis added).
16. Furman et al., *supra* note 9, at 80.
17. These challenges go beyond the traditional data security challenges that arise in making personal data accessible through technical means (although those challenges are, in and of themselves, quite substantial). The risk of inadvertent disclosure or data leakage inevitably grows as the ways to access systems increase. The complex, independent systems that are needed to implement data portability will necessarily create additional ways to access data and controlled services—which may translate to greater security risks to users. *See generally* John Palfrey & Urs Gasser, Born Digital: Understanding the First Generation of Digital Natives (2011).
18. *See* Art. 29 Working Party, *Guidelines, supra* note 11, at 5.
19. International Organization for Standardisation, ISO/IEC 19941:2017, *Information Technology – Cloud Computing – Interoperability and Portability* (2017), https://www.iso.org/obp/ui/#iso:std:66639:en.
20. *See* Facebook Decision and Order, *supra* note 13. *But see* Separate Statement of Commissioner Noah Joshua Phillips, *Federal Trade Commission v. Unrollme Inc.*, No. 1723139 (Aug. 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1539865/phillips_-_unrollme_statement_8-8-19.pdf (suggesting that Google's restriction of third parties from using the information in the Gmail accounts of consumers for purposes such as market research or advertising, while promoted as a means to enhance consumer privacy, may also limit consumer choice and competition).
21. *See* sources cited *supra* note 13.
22. Facebook Decision and Order, *supra* note 13.

23. *See, e.g.*, Ben Thompson, *The Bill Gates Line Follow-up, Twitter and the Bill Gates Line, Data Portability and Facebook*, Stratechery (May 29, 2018), https://stratechery.com/2018/the-bill-gates-line-follow-up-twitter-and-the-bill-gates-line-data-portability-and-facebook/ (acknowledging that "forced data portability and interoperability" would "return[] Facebook to the state it was with the original social graph API," which is what prompted Cambridge Analytica); Ben Thompson, *The Facebook Brand*, Stratechery (Mar. 19, 2018), https://stratechery.com/2018/the-facebook-brand/ (noting that Facebook Graph API allowed users to "give away everything about their friends" and "this is exactly how the researcher implicated in the Cambridge Analytica story" gained access to Facebook user data); Paul Przemysław Polański, *Some Thoughts on Data Portability in the Aftermath of the Cambridge Analytica Scandal*, 7 J. of Eur. Consumer and Market L. 141 (2018) (describing Cambridge Analytica as the result of flawed API implementation and calling for a conservative construction of the data portability right).
24. There are various technical means for accomplishing these transfers, and researchers are currently developing multi-lateral models that allow individuals to manage their data and decide where to store it. For example, personal information management systems ("PIMS") let individuals store their data either locally or via cloud-based storage and let them "define at a sufficiently granular level how their personal information should be used and for what purposes." *See* Eur. Data Protection Supervisor, EDPS Opinion on Personal Information Management Systems, Opinion 9/2016, at 7 (Oct. 20, 2016), https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf. In addition, an MIT project, "Solid," aims to create "decentralized social applications" that will allow individuals to move their information wherever they choose and switch between multiple platforms. *See* CSAIL-MIL, *What Does Solid Offer?*, Solid, https://solid.mit.edu/ (last visited May 22, 2019). The Data Mobility Infrastructure Sandbox began evaluating the viability of data portability facilitated by entities like PIMS earlier this year. *See* Ctrl-Shift, *Data Mobility Infrastructure Sandbox* (2019), https://www.ctrl-shift.co.uk/wp-content/uploads/2019/06/DMIS_June_2019_Downloadable_Singles_Final4.pdf.
25. Third parties who receive Covered Information through "a User-initiated transfer of Covered Information as part of a data portability protocol or standard" are not necessarily subject to the same controls and safeguards as third parties who receive Covered Information through other means. *See* Facebook Decision and Order, *supra* note 13.
26. GDPR, art. 20(1).
27. *See* Art. 29 Working Party, *Guidelines*, *supra* note 11, at 9.
28. The importance of ensuring that new requirements do not overburden smaller companies is a theme that has been sounded by many U.S. policymakers crafting privacy legislation. Several privacy bills contain certain exceptions for small entities. The DASHBOARD Act put forth by Sens. Mark Warner (D-VA) and Josh Hawley (R-MO), for example, limits its applicability to entities that "(1) generate a material amount of revenue from the use, collection, processing, sale, or sharing of the user data; and (2) have more than 100,000,000 unique monthly users in the United States for a majority of months during the previous 1-year period." *See* Press Release, Sen. Mark R. Warner, Warner & Hawley Introduce Bill to Force Social Media Companies to Disclose How They Are Monetizing User Data (June 24, 2019), https://www.warner.senate.gov/public/index.cfm/2019/6/warner-hawley-introduce-bill-to-force-social-media-companies-to-disclose-how-they-are-monetizing-user-data. As another example, in a recent hearing Rep. Jan Schakowsky (D-Ill.) noted that "[w]e must not lose sight of small and medium-sized businesses and how heavy-handed laws and regulations can hurt them. Established bigger companies can navigate a complex and burdensome privacy regime. But millions of dollars in compliance costs aren't doable for startups and small businesses." *See Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Prot. of the Comm. on Energy & Commerce*, 116th Cong. (2019) (statement of Rep. Jan Schakowsky, Subcomm. Chair). Similarly, EU policymakers have sought to avoid disproportionate burdens on small- and medium-sized enterprises by legislating exceptions to certain data protection obligations. *See, e.g.*, GDPR, art. 30(5) (exempting SMEs with 250 or fewer employees from certain GDPR record-keeping obligations). The GDPR also seeks to minimize disproportionate burdens on providers by permitting controllers to refuse to comply with data subject rights where requests are "manifestly unfounded or excessive, in particular because of their repetitive character." *See* GDPR, art. 12(5)(b).
29. *See, e.g.*, Dr. Aysem Diker Vanberg, *The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience*, 21(7) J. Internet L. 1, 3 (2018) ("[A]llowing one user to transfer a second user's information to another platform may violate the privacy rights of a second user."); Helena Ursic, *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, 15(1) SCRIPT-ed 42, 56 (2018), https://script-ed.org/wp-content/uploads/2018/08/ursic.pdf (noting "additional difficulties in applying the right to data portability" when data contains "multiple persons' data which are . . . intertwined"); Barbara Engels, *Data Portability Among Online Platforms*, 5 Internet Pol'y Rev., June 2016, 4-5, https://policyreview.info/articles/analysis/data-portability-among-online-platforms ("Allowing one to transfer a second user's information may violate the privacy rights of second user.").
30. *See* Comments of New America's Open Technology Institute, *In re* Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition, at 4 (F.T.C. Aug 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf [hereinafter OTI Comments] ("[N]owhere is [the tension between the right to portability and friends' right of privacy] greater than when it comes to the portability of information about your contacts on social networks, or your 'social graph.'").
31. *See, e.g.*, Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 Int'l Data PrivacyL. 74, 74–87 (2013), (supporting the idea of a property-based model of personal data that protects privacy); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2056 (2003), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1068&context=facpubs (developing a model of propertized personal information that protects privacy); *see also* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 Md. L. Rev. 335, 373 (2013) (suggesting that right to data portability

"appears more closely akin to the personal data ownership theory" than the right of access, and acknowledging debate around whether personal information is property).

32. *See, e.g.*, Hayley Tsukayama, *Knowing the "Value" of Our Data Won't Fix Our Privacy Problems*, Electronic Frontier Foundation (July 15, 2019), https://www.eff.org/deeplinks/2019/07/knowing-value-our-data-wont-fix-our-privacy-problems; Sarah Jeong, *Selling Your Private Information Is a Terrible Idea*, N.Y. Times (July 5, 2019), https://www.nytimes.com/2019/07/05/opinion/health-data-property-privacy.html.
33. *See Eur.* Commission, Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy; *see also* Cameron F. Kerry & John B. Morris, *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, Brookings Institution (June 26, 2019), https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.
34. Similar considerations could apply when determining how to address privacy issues in connection with business-to-business transfers of data (which, as noted above, are beyond the scope of this paper, but just as important to enabling competition as the individual right to data portability). In the context of these transfers, there are often additional factors present that can greatly impact the privacy issues around the transfer.
35. *See* Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, Electronic Frontier Foundation(July 24, 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine; Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, New America Weekly (June 28, 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends; *see also* Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, Eur. L. Rev. 793, 804-05 (2017) ("[T]he inability to access ["friends" data] could constitute a barrier to entry for potential competitors."). But *see* Thompson, *The Bill Gates Line Follow-up, supra* note 23.
36. *See, e.g.*, OTI Comments, *supra* note 30, at 4 ("Most services will now let you download your own social media posts, but what about other people's comments to those posts, or your comments and tags on other people's posts and photos? . . . . These are just some of the examples of the unresolved tension between my right to portability and my friends' right to privacy, and nowhere is that tension greater than when it comes to the portability of information about your contacts on social networks, or your 'social graph.'"); Lynskey, *supra* note 35, at 808 ("A further potential cost and complication for data controllers will be ensuring data security, given the tension between data security and data access. The A29WP perhaps underestimates the extent of this challenge for data controllers stating simply that the GDPR right may also 'raise some security issues' while highlighting that the data controller will remain responsible for 'taking all the security measures needed to ensure that personal data is securely transmitted[.]'"); Vanberg, *supra* note 29, at 7 ("The Article 29 Working Party arguably has not succeeded in offering more clarity as to what security standards are expected.").
37. *See* Art. 29 Working Party, *Guidelines, supra* note 11, at 19.
38. See Personal Data Protection Commission of Singapore, Discussion Paper on Data Portability 20 (Feb. 25, 2019), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf [hereinafter PDPC Discussion Paper].
39. *See* Personal Data Protection Commission of Singapore, Public Consultation on Review of the Personal Data Protection Act of 2012 – Proposed Data Portability and Data Innovation Provisions 17 (May 22, 2019) [hereinafter PDPC Public Consultation].
40. *See* Gennie Gebhart, *Bennet Cyphers & Kurt Opsahl, What We Mean When We Say "Data Portability,"* Electronic Frontier Foundation (Sept. 13, 2018), https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability; Bankston, *supra* note 35.
41. Notification fatigue is a problem often discussed in the breach notification context. *See, e.g.*, Jeri Clausing, *'Security Fatigue' Complicates the Battle Against Data Breaches*, Internet Soc'y (Dec. 21, 2016), https://www.internetsociety.org/blog/2016/12/security-fatigue-complicates-the-battle-against-data-breaches/; Christopher Mele, *Data Breaches Keep Happening. So Why Don't You Do Something?*, N.Y. Times (Aug. 1, 2018), https://www.nytimes.com/2018/08/01/technology/data-breaches.html.
42. *See* Bankston, *supra* note 35; *Josh Constine, Facebook Shouldn't Block You from Finding Friends on Competitors*, TechCrunch (Apr. 13, 2018), https://techcrunch.com/2018/04/13/free-the-social-graph; Cyphers & O'Brien, *supra* note 35; *see also* Lynskey, *supra* note 35, at 804-05 ("[T]he inability to access ["friends" data] could constitute a barrier to entry for potential competitors."). *But see* Thompson, *The Bill Gates Line Follow-up, supra* note 23.
43. *See* OTI Comments, *supra* note 30, at 6-7.
44. *Id.* at 7.
45. *See, e.g.*, sources cited *supra* note 13.
46. Art. 29 Working Party, *Guidelines, supra* note 11, at 19.
47. *Id.*
48. *See* PDPC Discussion Paper, *supra* note 38, at 20; Gus Rossi & Charlotte Slaiman, *Interoperability = Privacy + Competition*, Public Knowledge (Apr. 26, 2019), https://www.publicknowledge.org/news-blog/blogs/interoperability-privacy-competition ("[B]ecause they are dealing with personal data, third parties that want to interoperate would be required to follow a clear and transparent open model for user privacy, including potential requirements for pre-approval or certification by an independent entity.").
49. *See, e.g.*, GDPR, art. 42-43.
50. The Personal Data Protection Commission of Singapore recently proposed that it be given the power to issue binding codes of practice for sectors related to consumer safeguards, counterparty assurance, interoperability, and security of data. *See* PDPC Public Consultation, *supra* note 39, at 17 (the codes of practice would provide minimum standards for interoperability and security, criteria to verify the identity of recipient organizations prior to transfer, and information that must be provided to consumers to enable them to exercise their right to data portability).
51. *See* Art. 29 Working Party, *Guidelines, supra* note 11, at 6-7.
52. *See* Discussion Paper, *supra* note 38, at 20.
53. *See* PDPC Public Consultation, *supra* note 39, at 14.
54. Art. 29 Working Party, *Guidelines, supra* note 11, at 11.