Organisation for Economic Co-operation and Development

DAF/COMP(2020)1

Unclassified English - Or. English

29 April 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

# Consumer Data Rights and Competition - Background note

**by the Secretariat**

10-12 June 2020

This document was prepared by the OECD Secretariat to serve as background material for the meeting of the Competition Committee on 12 June 2020.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

More documentation related to this discussion can be found at:
http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm.

Please contact Mr. Antonio Capobianco if you have any questions about this document
[E-mail: Antonio.Capobianco@oecd.org]

**JT03461266**

# *Consumer Data Rights and Competition*

By the Secretariat*

*Consumer data rights are gaining more attention across the globe as more consumers come to rely on data-driven services in the digital economy. Consumer data rights can include fundamental rights to privacy, as well as a range of measures, such as data portability, that aim to provide consumers with greater control over their data.*

*This paper looks at the role for competition policy and enforcement in driving competitive outcomes in markets involving consumer data. Effective competition should theoretically drive better outcomes for consumers in terms of higher levels of privacy and control of personal data. However, it is not clear this is always the case, especially where consumers do not engage with consumer data rights, perhaps because of behavioural biases or a perceived lack of options. To this end, there is debate about whether and how competition enforcement should incorporate an assessment of the effects of the conduct in question on privacy and data protection outcomes. There are also questions about whether the possession of consumer data raises barriers to entry and whether there is a role for the essential facilities doctrine in addressing such issues. At the same time, some elements of consumer data rights, such as data portability, are intended to promote competition by facilitating comparison and switching. However, it is not clear how best to implement these measures in order to best promote competitive outcomes.*

*This paper aims to address these issues and ultimately finds that there is a role for competition policy and enforcement in promoting better consumer outcomes in markets involving consumer data. Ideally, this should be pursued in co-operation with government agencies responsible for data protection, as well as consumer policy and enforcement.*

* This paper was prepared by Anna Barker of the OECD Competition Division. The document benefitted from comments from Antonio Capobianco, Pedro Caro de Sousa, Pedro Gonzaga, Chris Pike, and Ania Thiemann (all of the OECD Competition Division).

# *Table of contents*

## Tables



### Figures



### Boxes

# 1. Introduction

1. The digital transformation is changing our economies and societies, powered partly by the collection and use of ever-growing quantities of consumer data. Data has never been so prevalent – the volume of data produced globally is forecast to grow from 33 zettabytes in 2018 to 175 zettabytes in 2025 (European Commission, 2020[1]). To put this in perspective, one zettabyte is equivalent to about 250 billion DVDs (Arthur, 2011[2]). Further, we are seeing an *"emergence of a global data ecosystem in which data and analytic services are traded and used across sectors and national borders"* (OECD, 2015, p. 24[3]).

2. A range of businesses now rely on the consumer data that they collect as consumers use the Internet, digital applications (apps) and Internet of Things (IoT) devices. In this context, the use of consumer data has brought, and will continue to bring, a wide range of new and innovative goods, services and business models, often at a zero (monetary) price. Further, the analysis of consumer data, alone or when combined with other data, by artificial intelligence (AI) systems, can produce new predictions and be used to glean new insights across a range of issues. While the benefits to consumers are clear, business use of consumer data also raises concerns, such as how to preserve privacy and ensure that businesses and other actors do not use consumer data in ways that disadvantage consumers. In response, a number of OECD countries have recently enacted, or are considering enacting, new consumer data rights to further protect privacy and improve consumers' control of their data.

3. Business models based on the collection and use of consumer data also raise new questions for competition policy. For example, in markets where businesses compete on privacy, how should competition authorities incorporate this into competition assessments? In addition, when and how might consumer data raise barriers to entry or expansion, and when might consumer data be an essential input for complementary, competing or downstream businesses? Further, how do business and regulatory decisions regarding the collection, storage and use of consumer data impact on competition and the broader economy?

4. This paper considers these questions and reviews the impacts of consumer data rights and the use of consumer data more broadly on competition policy and enforcement.

## 1.1. Past OECD work

5. This paper builds on work already undertaken by the Competition Committee, as well as work done across the OECD, especially in respect of privacy and data protection, as outlined below.

### *1.1.1. Work of the Competition Committee*

6. Issues relating to consumer data were first considered by the Competition Committee in a November 2016 hearing on "Big Data" (OECD, 2016[4]). Among other things, this introduced the concept of big data, described the big data ecosystem and looked at implications for competition law enforcement. In the years since, there have been a number of regulatory, market and competition law developments, which suggest that it is timely to revisit these issues more specifically in the context of consumer data.

7. Consumer data was also relevant to a number of roundtables held in 2018. In particular, privacy may be relevant to competition where it is an aspect of the quality of a given good or service. In this context, privacy, including competition around the levels of

privacy afforded by businesses, was touched on in the roundtable on "Non-price Effects of Mergers" in June 2018, and the roundtable on "Quality Considerations in the Zero-price Economy" in November 2018 (OECD, 2018[5]; OECD, 2018[6]). The collection and use of consumer data was also discussed in the roundtable on "Personalised Pricing in the Digital Era", since the increased use of consumer data and improvements in analytics have given rise to concerns about the ability of businesses to engage in personalised pricing, especially in digital markets (OECD, 2018[7]). Issues around privacy were also relevant to the discussion on "Digital disruption in financial markets", which took place at the OECD's Competition Open Day in February 2020 (OECD, 2020[8]).

8. Two other roundtables scheduled for the June 2020 Competition Committee meetings are also relevant to consumer data and competition. These are a roundtable on "Start-ups, killer acquisitions and merger control" and one on "Conglomerate effects of mergers" (OECD, 2020[9]; OECD, 2020[10]).

### *1.1.2. Other OECD work*

9. The OECD has played a pioneering role in shaping privacy and data protection policies across its member states. The OECD's "Privacy Guidelines", first agreed in 1980, were the first international set of privacy principles for the protection of personal data across the public and private sectors. The minimum standards set out in the Guidelines have influenced legislation and policy in OECD Member countries and beyond. The Guidelines were reviewed in 2010, and revised in 2013 to reflect significant changes to the role of personal data in the economy over the intervening years (OECD, 2013[11]).

10. The Guidelines set out eight basic principles, including collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The Guidelines also focus on the practical implementation of privacy protection and increased efforts to address the global dimension of privacy through improved interoperability. They also modernise the approach to trans-border data flows, flesh out the principle of accountability, and strengthen privacy enforcement. The OECD Digital Economic Policy Committee's (CDEP) Working Party on Data Governance and Privacy (WPDGP), part of the Directorate for Science, Technology and Innovation (STI), is currently reviewing the Guidelines, with the outcomes of the review expected by the end of 2020.

11. In addition, the WPDGP is currently undertaking a project on "Data Portability", which will consider the competition impacts of data portability, among other things, drawing on relevant theory and evidence. The project is expected to run through 2020 and possibly into 2021. Other STI publications that are particularly relevant to the current topic include a 2015 report on "Data-Driven Innovation" and a 2018 report on "Enhancing Access to and Sharing of Data" (OECD, 2015[3]; OECD, 2019[12]). In particular, these two reports provide a good overview of how the various players collect, analyse and use data across the economy, as well as identifying obstacles to greater sharing of data.

12. In addition, the OECD's Committee on Consumer Policy has released a "Good Practice Guide on Consumer Data", which provides a consumer policy and enforcement perspective on the issue of consumer data, especially where businesses have engaged in misleading or deceptive conduct, or unfair practices, in respect of consumer data (OECD, 2019[13]). This is discussed in more detail in Section 5.2.

## 1.2. Structure

13. This paper starts by defining consumer data and providing an overview of the various types of consumer data rights (Section 2). Section 3 discusses how businesses

collect and use data, as well as their incentives for sharing data. It also discusses possible market failures associated with businesses collecting and using consumer data. Section 4 then considers the role for competition law enforcement in promoting privacy and assessing competition in markets involving consumer data. Specifically, it looks at possible theories of harm, analytical challenges (including market definition, barriers to entry, consumer attitudes towards privacy, measuring data protection, and efficiencies), potential remedies and a possible role for the essential facilities doctrine. Section 5 then discusses the way that data rights effect competition and the need for cooperation between relevant regulatory authorities. Section 6 then presents some conclusions.

## 2. What are consumer data and consumer data rights?

14. This section provides a working definition of consumer data, discusses consumer data typologies, and provides an overview of the various types of consumer data rights available across the various OECD member countries.

### 2.1. What is consumer data?

15. The term "consumer data" is intended to capture data concerning consumers, where such data have been collected, traded or used as part of a commercial relationship.

16. This is in some ways narrower than the concept of "personal data", which is "*any information relating to an identified or identifiable individual (data subject)"* (OECD, 2013, p. 13[11]). That is, "personal data" encompasses individuals' data as they relate to the individual, both as a citizen and consumer. However, the concept of consumer data used in this paper applies only to data relevant to an individual as a consumer since competition policy and enforcement is concerned with commercial transactions. That is, "consumer data" does not include data that are collected, traded and used by governments, or other non-commercial agents or organisations, which may raise different issues.

17. The term "consumer data" is also broader than "personal data" since it may also capture data concerning consumers even where such data cannot necessarily be traced to the individual. While such data may not raise the same concerns under privacy and data protection law, which predominately relate to "personal data", they may be relevant to the competition assessment, as will be discussed in more detail in Section 4 in particular.

### 2.2. Consumer data typologies

18. Consumer data are heterogeneous (Crémer, de Montjoye and Schweitzer, 2019[14]) and the private and social value of data depends on how it is used, and can vary for different players in the value chain (Acquisti, Taylor and Wagman, 2016[15]). Hence, understanding the various dimensions of consumer data is important to understanding the potential value of different types of consumer data. In this respect, there are a number of ways to classify consumer data. This can include: (i) by the type of data collected, (ii) by the origin of the data, or (iii) according to whether consumer data can be personally identifiable. Each of these classifications are discussed briefly below.

19. One way to classify data is by the type of information collected (Robertson, 2020[16]; Kemp, 2019[17]; OECD, 2013[18]), including:

- **User generated content**, including blogs and commentary, photos and videos, as well as communications with others.

- **Activity or behavioural data**, including what people search for online, what websites they visit, what apps they use, what people buy online, how much and how they pay, as well as habits and preferences. IoT products may also collect information such as conversations, and health related data, such as heartrate, sleep and exercise (see Box 1).
- **Social data**, including contacts and friends on social networking sites and on communication apps.
- **Locational data**, including residential addresses, GPS and geo-location (e.g. from cellular mobile phones), IP address, as well as proximity to other individuals.
- **Demographic data**, including age, gender, race, income, sexual preferences and political affiliations.
- **Identifying data of an official nature**, including name, financial information and account numbers, health information, national health or social security numbers, police records.
- **Biometric data**, including for example, fingerprints, face recognition, eye recognition and voice recognition.

20. This demonstrates the wide variety of consumer data that businesses collect and use. It also highlights some of the privacy sensitivities associated with such data.

### Box 1. The Internet of Things

The OECD defines the Internet of Things (IoT) as:

> *... all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals.*

Moreover, the IoT includes objects and sensors that gather data and communicate these data with one another and with individuals. This communication, combined with cloud services, remote operation and analytics, is what makes these types of applications "smart". The underlying IoT technologies include semi-conductors (i.e. sensors, chips, processors and memory); modules and devices (i.e. software); IoT platforms (i.e. the operating systems), and the network (i.e. connectivity where standardisation and interoperability issues are relevant).

Some of these connected devices will be in private residences, providing functions such as energy management, security or entertainment. Others will be associated with developments in areas such as transport, health and manufacturing. The number of connected devices in and around people's homes in OECD countries is forecast to grow from one billion in 2016 to 14 billion by 2022. Worldwide, the total installed base of IoT connected devices is projected to reach 75.44 billion by 2025. This represents a fivefold increase in ten years. These devices are a key source of data that are feeding big data analytics, and much of this data is consumer data. Such data can include consumers' conversations, location, home address, entertainment and fitness habits, and physiological signs, for example.

Sources: OECD (2015[19]); OECD (2017[20]); OECD (2018[21]); Statistica (2020[22]).

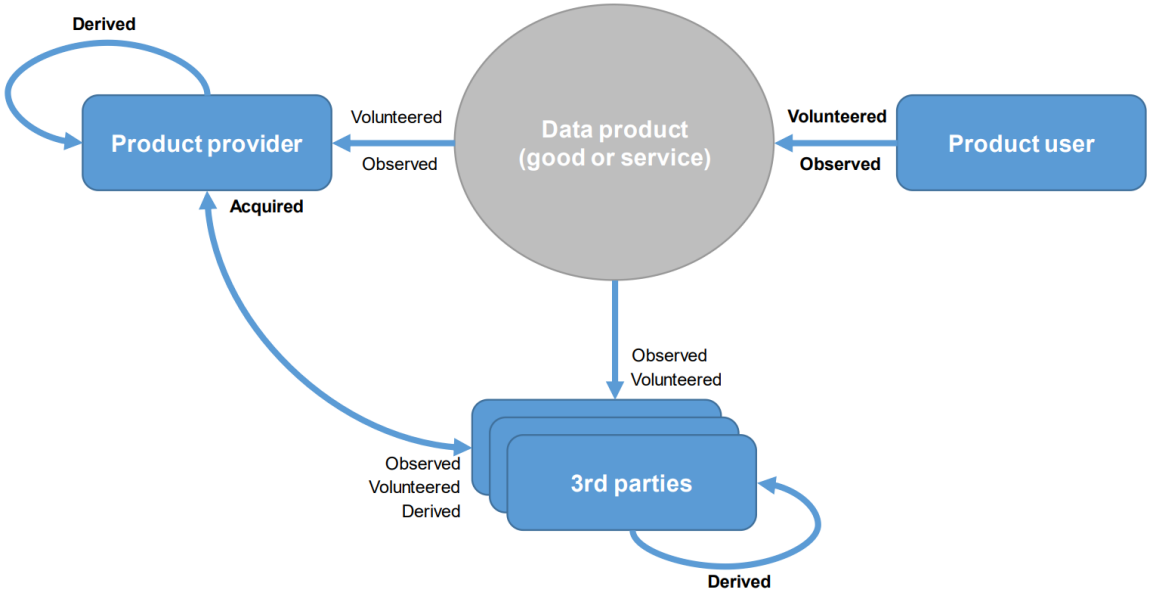
### *2.2.1. Origin of data*

21. Consumer data can also be categorised according to their origin. In this respect, the OECD (2019[12]) has proposed the following four categories:[1]

1. **Volunteered data** are data that individuals provide when they explicitly share information about themselves or others. Examples include log in credentials, social media posts, and credit card information for online purchases.
2. **Observed data** are created where an individual's activities are captured and recorded. Individuals create this data passively and sometimes unknowingly. Examples include location tracking and online browsing activities.
3. **Derived (or inferred) data** are created from data analytics, including data that is derived mechanically from other data, as well as from more sophisticated techniques. Credit scores are one example. The individual is likely unaware of this data, and such data can be inferred even without much information being provided by the individual.
4. **Acquired (purchased or licenced) data** are obtained from third parties through commercial licensing contracts (e.g. from data brokers) or non-commercial means (e.g. open government initiatives). Contractual and other legal obligations may affect the re-use and sharing of such data.

22. The flows between these categories of consumer data are shown in Figure 1.

**Figure 1. Types of consumer data, according to how data are generated**




Source: OECD (2019[12])

23. The policy relevance of this typology is twofold. First, how data originates will affect consumer awareness of the data, and consumer awareness is important to addressing asymmetric information problems associated with the collection and use of consumer data.

[1] This approach combines the approach of Adams (2014[180]) and the Productivity Commission (2017[182]). It is also consistent with that applied by Crémer, de Montjoye and Schweitzer, in their report on Competition Policy for the Digital Era, for the European Commission (2019[14]).

In particular, consumers will be most aware of data that they have volunteered, may have some awareness of observed data, and will have less awareness of derived and acquired data. Second, volunteered (and potentially observed data) is arguably less subject to business claims that the data has been "created" by the business, than derived and acquired data. This is relevant to the incentives of businesses to share these various types of data, as well as the effect of policies relating to data portability and interoperability which may need to balance trade-offs between stimulating competition and protecting incentives for investment, not to mention third-party privacy concerns. These issues are discussed in more detail in Section 5.1.1.

### *2.2.2. Identification of personal data*

24. Personal data can also be classified according to the extent to which it is personally identifiable. In particular, ISO/IEC 19441 distinguishes between five categories including:

1. **Identified data**, which is unambiguously associated with a specific person.
2. **Pseudonymised data**, in which aliases are used in place of personal identifiers; aliases can only be reversed by the party that assigned them.
3. **Unlinked pseudonymised data**, in which all identifiers are erased or substituted by aliases for which the assignment function is erased or irreversible, so that the linkage cannot be re-established by anyone.
4. **Anonymised data**, which is unlinked and altered (e.g. attributes' values are randomised or generalised) in such a way that there is a reasonable level of confidence that a person cannot be identified.
5. **Aggregated data**, which does not contain individual-level entries and is combined from information about enough different persons that individual-level attributes are not identifiable (ISO/IEC, 2018[23]).

25. The relevance of this categorisation is that where data cannot be attributed to an individual, the data is less likely to trigger privacy laws. Hence, such data may be able to provide economic and competitive benefits without triggering offsetting privacy concerns (OECD, 2019[12]). In practice, however, is may be difficult to safeguard anonymous data against re-identification (PCAST, 2014[24]). Further, externalities associated with consumer data (see Section 3.4.2) may mean that even unidentified data may be combined with identified data to gain insights about individuals or to facilitate personalised pricing, for example.

### *2.2.3. The four Vs*

26. Consumer data can also be discussed in terms of the four 'V's: volume, velocity, variety and value (OECD, 2016[4]; Stucke and Grunes, 2016[25]). In particular, the **value** of data, especially in respect of the accuracy of predictions (which can help improve goods and services as well as better target advertising to increase advertising revenues – see Section 3.3.1) has increased substantially due to increases in the volume, velocity and variety of data (Gal and Rubinfeld, 2019[26]):

- Two key factors have led to substantial increases in the **volume** of consumer data available, including:
  - Decreasing costs of collecting, storing, processing and analysing data.
  - The increasing online activity of consumers, driven by increased access to high speed Internet, as well as more online and connected goods and services, including those provided by IoT devices (see Box 1) (OECD, 2015[3]).

- These same factors have led to an increase in the **velocity** at which data are generated, accessed, processed, and analysed. Some businesses are now able to make predictions in real-time (called "nowcasting") (Stucke and Grunes, 2016[25]).
- The **variety** of data also influences its value. This can be especially important for consumer data in that greater variety allows for greater accuracy in respect of personalisation, be it recommendations, offers, or targeted advertising (Stucke and Grunes, 2016[25]).

27. Since the volume, velocity and variety of data are important to its value, they may be relevant considerations for competition assessments involving data-driven businesses. For example, this framework may be useful when assessing a merger that involves a merging of data assets, or when assessing whether a business' access to data creates barriers to entry or provides them with a competitive advantage (see Section 4.2.2).

## 2.3. Consumer data rights

28. This section provides a broad overview of the types of consumer data rights that apply across OECD member countries. In particular, it introduces the broad privacy framework applied across the OECD, as well as noting some of the specific rights afforded to individuals from OECD member countries.

### *2.3.1. General rights*

29. Most OECD member countries have some form of data protection legislation in place, consistent with the framework set out in the OECD's "Privacy Guidelines", and the eight principles outlined in Box 2 (OECD, 2013[11]). Such legislation tends to provide basic privacy protections as well as affording rights to data subjects to better control their data. In particular, most jurisdictions operate a consent-based regime, which provides consumers the ability to control how their data are collected and used by agreeing or withholding their consent. In addition, in some jurisdictions, data protection legislation confers other rights including:

- the right to correct false information, which provides data subjects the right to have incorrect personal information corrected by the data controller
- the right to be forgotten, which provides data subjects the right to have personal data deleted
- the right to data portability, which provides data subjects the ability to move their personal data from one "data controller" to another.

30. Such rights are included in Europe's main data protection legislation, the General Data Protection Regulation (GDPR), as outlined in Box 3. Similar rights exist in some states of the United States, such as in California under the California Consumer Privacy Act (CCPA).

31. Data rights are currently state based in the United States, though the Federal Trade Commission (FTC) has authority to ensure that businesses do not engage in unfair or deceptive acts or practices, including in respect of data practices (see also Section 5.2). Further, federal legislation is currently under consideration. For example, the DASHBOARD Act, which would require data collecting platforms to improve transparency about data collection and use, and the "Own Your Own Data Act", which would give users an exclusive property right to their online data, are currently under consideration (Chakrovorti, 2020[27]). In addition, the ACCESS Act, which would require

data portability for social media platforms with over 100 million users in the United States, is currently being considered.

### Box 2. OECD privacy principles

The OECD's eight privacy principles include:

1. **Collection limitation:** There should be limits to the collection of personal data and data should be obtained by lawful and fair means with the knowledge or consent of the data subject.
2. **Data quality:** Personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete, and kept up-to-date.
3. **Purpose specification:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use should be limited to these purposes.
4. **Use limitation:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: a) with the consent of the data subject; or b) by the authority of law.
5. **Security safeguards:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
6. **Openness:** There should be openness about data collection and use practices to allow individuals to establish the existence and nature of personal data, data use, as well as the identity and residence of the data controller.
7. **Individual participation:** An individual should have the right:
    a. to know whether a data controller has data relating to him or her
    b. to receive their data (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible
    c. to be given reasons if a request is denied, and to be able to challenge a denial
    d. to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
8. **Accountability**: A data controller should be accountable for complying with measures, which give effect to the principles stated above.

Source: OECD (2013[11]).

32. Australia's *Privacy Act 1988* similarly confers a range of rights on individuals including rights to know what personal information is being collected, how it will be used and who it will be disclosed to; the option to not identify yourself; to request access to personal information; and a right to correct incorrect personal information. Further, new legislation enacted in 2017 established a "Consumer Data Right" to facilitate data portability (this is discussed in more detail in the next section). Some other examples of relevant legislation include the *Privacy Act 1993* in New Zealand, and the *Personal Information Protection and Electronic Documents Act (PIPEDA)* and *Privacy Act* in Canada.

### Box 3. Europe's General Data Protection Regulation (GDPR)

The GDPR includes a number of rights for European citizens, including rights to:

- access personal data (Art. 15)
- rectify inaccurate personal data (Art. 16)
- be forgotten (Art. 17)
- data portability (Art. 20)
- not be subject to automated decision making, including personal profiling, subject to exceptions (Art. 22).

Other key aspects of the GDPR include:

- a revised and broadened definition of personal data (Art. 4)
- strengthening of the consent regime as applied to the collection and processing of personal data (Art. 6 and Art. 7)
- a requirement that privacy policies be transparent and easily accessible (Art. 12, Art. 13 and Art. 14)
- wider territorial scope (Art. 3).
- a requirement for data protection by design and by default (Art. 25)
- greater enforcement fines (Art. 83).

Sources: GDPR; CMA (2015[28]); Moazed (2019[29])

#### *2.3.2. Data portability*

33. Data portability has been proposed as a way of improving "informational self-determination", as well as competition outcomes, for example, by facilitating switching (EDPS, 2014[30]). There are a number of government-initiated voluntary data portability initiatives, as well as legislated rights across the OECD member countries.

34. The "My Data" initiatives, which the US Government enacted in 2010, are one example of a set of voluntary initiatives. Some of these facilitate access to information held by government agencies (Honey, Chrousos and Black, 2016[31]). For example, the "Get Transcript" initiative streamlines access to data held by the Internal Revenue Service, and the "My Student Data" initiative provides access to federal student data. There are also initiatives to facilitate access to data held by private businesses. These include the "Green Button" initiative for electricity utility data, and the "Blue Button" initiative for health data held by public and private sector health care providers (United States Department of Energy, n.d.[32]).

35. In the United Kingdom, the government introduced its Midata data portability initiative in 2011, which seeks to give consumers access to the electronic information that companies hold about their transactions in a machine-readable and portable format (Department for Business, Innovation & Skills, 2011[33]). The Midata initiative focuses on consumer information in the energy, mobile phone and financial sectors. In addition, since January 2018, all UK banks have been required to comply with the Open Banking rules, which facilitate data portability in the UK financial sector (Open Banking, n.d.[34]).

36. In addition, a number of OECD member countries have created data portability rights. Some examples are provided in Box 4.

### Box 4. Data Portability Rights

In 2017, the **Australian Government** announced the introduction of a consumer data right (CDR) to give consumers and small businesses greater access to and control over their data. Its purpose is to drive competition by facilitating easier comparison and switching between competing suppliers through data portability. The CDR, which focuses first and foremost on the consumer experience, aims to alter the economic landscape over time by facilitating the use of data for new entrants across a wide number of sectors. The CDR will first apply to the banking sector, followed by the energy sector, with the telecommunications sector proposed to follow. There will be a phased introduction. The ACCC is the lead CDR regulator, alongside the Office of the Australian Information Commissioner (OAIC) and the Data Standards Body (DSB).

In **Europe**, Article 20 of the GDPR, which came into force in 2018, provides Europeans with the right to receive and transfer their personal data in a "structured, commonly used and machine-readable format". The right applies to all volunteered and observed personal data processed by automated means in relation to the performance of a contract. However, exercising this right should not adversely affect the rights and freedoms of others (e.g. the privacy of others). Also in Europe, the Payment Service Directive for Payment Businesses (PSD2) requires banks to allow third parties to access customers' payment account data subject to the explicit consent of customers.

The **California** Consumer Privacy Act (CCPA), which came into effect at the start of 2020, merges the right to access and the right to data portability. It gives consumers the right to request businesses to disclose to them the categories and specific pieces of personal information the business has collected about them. In addition, consumers can ask businesses for information on the business or commercial purposes for collecting or selling personal information, details of the categories of third parties with whom the business shares or sells the personal information, and categories of personal information sold or disclosed for a business purpose.

Sources: ACCC (n.d.[35]); OECD (2019[12]); *General Data Protection Regulation (EU) 2016/679*; *California Consumer Privacy Act*; Takatsuki (2019[36]).

## 3. How and why businesses collect and use consumer data

37. Businesses collect and use consumer data in a number of different ways, as will be discussed in this section. In addition, this section will discuss the incentives on businesses to collect and share consumer data, and possible market failures associated with the collection and use of consumer data.

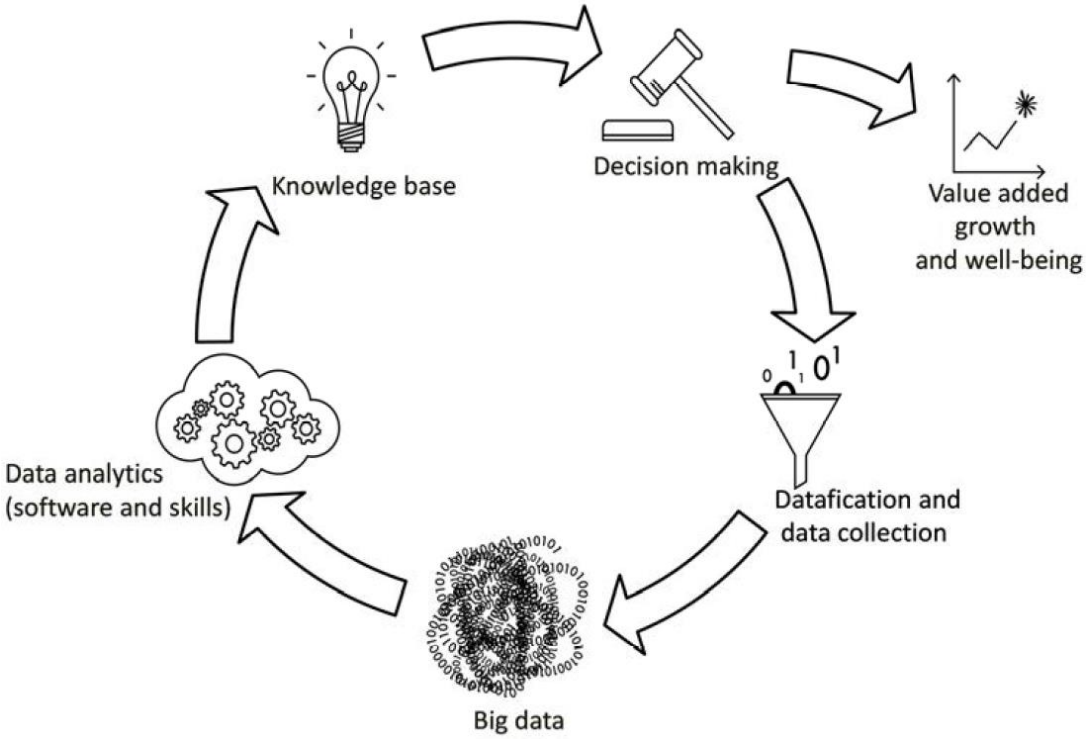
38. The OECD's report on "Data-Driven Innovation" sets out the following phases in the data value cycle:

- "Datafication" and data collection – data generation through the digitisation of content, and monitoring of activities, including real world (offline) activities and phenomena, through sensors (e.g. involving the IoT).

- Big data – the result of datafication and data collection that leads to a large pool of data that can be exploited through data analytics.
- Data analytics – to infer meaning from the data; data analytics is increasingly undertaken via cloud computing.
- The knowledge base – the knowledge that is accumulated through learning over time, including through machine learning and Artificial Intelligence (AI) systems.
- Data-driven decision making – where decisions are made on the basis of the use of the data, data analytics and the knowledge base (OECD, 2015[3]).

39. These phases are shown in Figure 2.

**Figure 2. The data value cycle**




Source: OECD (2015[3])

40. As far as the competition impacts go, the production chain can be simplified to data i) generation and collection and ii) analysis and use. These are discussed below.

## 3.1. Data generation and collection

41. In general, consumer data can be viewed either as a by-product of a business' core functions, or as something that a business has actively pursued alongside or even separate to its core business (Rubinfeld and Gal, 2017[37]). That is, data collection may be passive or active. In some cases, data collection may have started as a passive activity where a business did not yet appreciate the value of such data. For example, retail businesses took a while to understand the value of retail scanner data (Turow, 2017[38]). However, once retail businesses understood this value, many created fidelity or loyalty schemes to collect great masses of consumer data (see Box 5). Similarly, Google did not originally appreciate the (profit generating) value of consumer data collected in respect of its search services,

but now this is one of its greatest assets (Zuboff, 2019[39]). In many cases, once businesses start to understand the value of by-product data, they tend to move from passive to more active data collection practices.

### Box 5. Fidelity schemes

Many businesses have fidelity or loyalty schemes, which offer consumers benefits in terms of points, discounts or other offers, in exchange for (often zero-price) membership and use. Airlines, banks, cinemas, hotels, restaurants and retailers, for example, often offer these types of schemes. Primarily, these types of schemes are a marketing device designed to attract and retain customers. However, businesses are increasingly using these schemes to collect consumer data, which can be used to develop consumer insights and to target advertising. As an example, Tesco, a UK supermarket chain, collects vast quantities of data through its fidelity card scheme. Such data represents over 100 "shopping baskets" a second, and over six million transactions per day, and has arguably brought considerable value to the business.

In 2019, the ACCC undertook a review of customer loyalty schemes, which raised a number of consumer policy concerns regarding how businesses collect and use consumer data associated with the use of customer loyalty schemes. In particular, the ACCC was concerned, under its consumer policy remit, that consumers have little control over how businesses use such data, and about the lack of clarity provided to consumers regarding the collection and use of consumer data. Consumer understanding of data collection practices is discussed in more detail in Section 4.2.3.

Sources: ACCC (2019[40]); OECD (2015[3])

#### *3.1.1. First party versus third-party data collection*

42. When talking about the collection of consumer data, it is useful to distinguish between first and third party data collection. First party data collection occurs where a business collects information directly from its customers/users as part of their use of the business' goods or services. For example, Google's first party data is the data that Google collects from users when they are using Google search, Google photos, Gmail and other services owned and provided by Google. In comparison, Robertson (2020, p. 162[16]) defines third-party tracking as:

> *…a practice which allows a tracker to harvest extensive amounts of personal data from a variety of first-party sources in the online environment and across different devices such as smartphones, tablets and laptops/computers, ultimately building a comprehensive user profile.*

43. To continue the example above, in addition to the data it collects on its own websites and applications, Google also collects a wide range of data from third-party tracking of consumers on a range of (non-Google) websites and apps (Robertson, 2020[16]). Third parties may agree to such tracking as part of commercial agreements to receive website analytics and ad serving services, for example, as well as in using proprietary Application Programming Interfaces (APIs) (discussed more in Section 5.1.1). Third-party tracking is facilitated through a range of different technologies (see Box 6).

### Box 6. Tracking technologies

Traditionally, "cookies" (essentially digital code that records certain user behaviour) were used to track online behaviour via desktop browsers. Cookies can be first-party or third party. First-party cookies originate from (or are sent to) the website the consumer is currently viewing, whereas third-party cookies originate from (or are sent to) an unrelated website. However, cookies are less effective at tracking online activity on mobile devices. This is because cookies are not necessarily shared between mobile apps, and some mobile browsers, such as Safari, block third-party cookies by default.

As consumers now tend to use a range of devices to access online services, businesses are using other means to track individuals online. These methods can be categorised as "deterministic" or "probabilistic". Deterministic methods use consumer identifying characteristics, such as log ins, to track consumers across devices. Probabilistic methods instead infer an consumer's identity through means such as IP address (since a computer, smartphone, and tablet that use the same public IP address are likely to belong to the same household); geolocation information; browser or device fingerprinting; and general usage patterns. US Federal Trade Commission (FTC) staff found that, of 100 popular websites used across two devices: at least 87 used cross-device tracking; 96 allowed consumers to submit a username or email address; and 16 shared user names or emails with third parties.

In addition, businesses are increasingly using tracking pixels to facilitate third-party tracking. Pixels are small (essentially invisible) graphics that embed a piece of code that is loaded when a user visits a webpage or opens an email. Similar to cookies, pixels facilitate tracking by registering certain actions and noting these in the server's log files.

Sources: Beal (2008[41]); IAB (2013[42]); FTC (2017[43]); Boerman et al. (2017[44]); OECD (2019[45]); Ryte (2019[46]).

44. Third-party tracking is prevalent across both websites and apps for mobile devices. In 2018, there was at least one third-party tracker on 95% of the top 10 000 websites and over 90% of the free apps on the Google Play store (Binns et al., 2018[47]; Purra and Carlsson, 2016[48]). However, while many players engage in tracking, *"the majority of these trackers are controlled by a small number of data giants"* (Ezrachi and Roberston, 2019[49]). Alphabet/Google holds first spot for both apps and websites. Facebook and Twitter also hold strong positions across websites and apps, though Microsoft (including LinkedIn) takes second place in respect of apps (Binns et al., 2018[47]; Purra and Carlsson, 2016[48]). That said, some 18% of the free apps on the Google Play store contained over twenty different trackers (Binns et al., 2018[47]).

45. As discussed above, the way in which consumer data is collected has implications for privacy and competition. This applies not only to how the consumer provides the data (or the business creates the data) but also to who the consumer provides the data to. In respect of privacy, consumer awareness of data collection practices influences their ability to control their personal data. Specifically, consumers may feel most comfortable in relation to volunteered data that is collected and used directly by first parties. They might also feel relatively comfortable in respect of first party observed data. However, consumers may be less aware of data gathered through third-party tracking, even where consumers provide such data voluntary or where they are aware that their data is being observed by the relevant (first party) business. In particular, consumers may willingly provide information in one context that will then be used in another context that the consumer would

otherwise object to if they were fully aware of this. This is because the consumer's value from keeping personal information private, or sharing it, is highly context specific (Acquisti, Taylor and Wagman, 2016[15]). Such issues are also relevant to competition: if consumers do not understand how their data is being collected and used, then they are less likely to be able to drive effective competition in respect of this (see also Section 4.2.3).

46. A business' ability to recreate or otherwise access similar consumer data as that held by a competitor will also be a relevant consideration in a number of scenarios but especially when considering whether a business holds a dominant position or whether access to a competitor's data might be a pre-cursor to effective competition (see also Sections 4.2.2). That is, even where certain consumer data is easily collected in various ways and by various parties, access to third-party tracking, as well as a large and individually identifiable consumer base, may provide a business with a particularly valuable set of data that may be difficult for competitors to replicate. Binns and Bietti (2019[50]) argue that not enough attention has been paid to third party tracking in competition cases, especially in mergers between firms that are active in third-party tracking. This is discussed in more detail in Section 4.

### *3.1.2. Storage*

47. Business decisions regarding how and where data is stored also influence privacy and competition outcomes. For example, decisions about whether personal data collected from an IoT device is stored on the device or externally (e.g. with the manufacturer or in the cloud), will affect privacy and competition. Data that is stored locally on a consumer's device, that is not accessible by any other parties without explicit consent, is less likely to raise privacy concerns. However, the broader social benefits that could potentially arise from the analysis and use of this data may not be realised, including competition that could arise from wider use of the information (e.g. competition to offer a loan knowing a consumer's credit score). On the other hand, data held by the manufacturer or in the cloud, has more potential to raise privacy concerns. Further, if businesses do not share data more broadly, again, this may limit the societal benefits that could arise from more widespread use of the data. An example of these issues as they relate to connected cars is provided in Box 7.

#### Box 7. Data governance in connected cars

Connected and automated cars generate a range of data including technical data, weather and traffic data, as well as data about driving behaviours, location, and the entertainment and navigation preferences of the owners, for example. Through connectivity, such data can be transmitted in real time to external entities. This data is useful not only for the manufacturer, but also for providers of aftermarket and complementary services (for example, navigation, entertainment and insurance services).

Connected and automated cars can bring a variety of benefits for consumers and society more generally. One key issue in realising these benefits is to ensure that appropriate data governance arrangements are in place to manage access to and control of in-vehicle data (including consumer data). There has been debate about how best to achieve this. As noted by Kerber (2019[51]), car manufacturers have tended to advocate for an "extended vehicle concept" which would involve transmitting all data back to the original equipment manufacturer (OEM) for their exclusive use. Independent service providers (ISPs) on the other hand, have argued for non-discriminatory access via a "shared server" solution or, in the longer term, the development of an "on board

application platform". The latter would allow consumers to decide where their data are stored and who they allow to access the data.

These proposals have different impacts for competition. In theory, competition between OEMs could be expected to drive competition in aftermarket services. However, Kerber (2019[51]) finds that in practice, consumers tend not to be very good at factoring in aftermarket services when buying cars. Further, he finds that competition between OEMs cannot solve market failures associated with choosing the optimal technologies concerning technical standards and interoperability. Hence, the "extended vehicle concept" is unlikely to facilitate competition in markets for aftermarket and complementary services. In comparison, the proposals from ISPs are more likely to foster competition in related markets, though if OEMs retain control of access under the "shared server" proposal, they could potentially block access by potential competitors, with consequences for competition.

OEMs have argued their position on the basis of safety and security considerations. However, research by Kerber (2019[51]) suggests that these concerns cannot justify the exclusive control of data by OEMs. Overall, Kerber (2019[51]) suggests that while all solutions have advantages and disadvantages, the "on-board application platform" offers the highest potential benefits. In particular, this solution appears to both allow consumers to control their data and manage privacy whilst also facilitating competition.

Source: Kerber (2019[51]).

## 3.2. Analysis and use

48. Declining costs of data storage and processing have facilitated improved and more affordable data analytics, especially through cloud computing (OECD, 2015[3]). There are a number of ways in which businesses can use consumer data, including, by using the data internally to:

- increase the quality or functionality of their core products or services
- offer greater personalisation (including, possibly, personalised pricing or offers)
- train machine learning and other forms of analysis underpinning AI systems (see Box 8)
- sell advertising products or other targeted services, usually involving two-sided or multi-sided markets.

49. In addition, businesses can sell consumer data to third parties (potentially subject to consumer approval or anonymization, depending on the regulatory regime in place) (Gilbert and Pepper, 2015[52]). Markets for consumer data and consumer reports have existed for some time. However, such markets are complex and tend to be decentralised and there are many different business models and players involved (CMA, 2015[28]).

50. Given these various uses, consumer data can have substantial economic value, which provides an incentive for businesses to collect ever-greater volumes of consumer data. As noted by Kemp (2019, p. 10[17]):

> *Suppliers have been enjoined to "measure everything" in the interests of customer profiling, targeted marketing, customisation, price discrimination, risk analysis and to support other potential applications of artificial intelligence in their businesses. For these purposes, on one view, more data is better. Machine learning*

*is data hungry. Competitors are benefiting from millions of "insights" about consumers in the market and possibilities of extending into other markets.*

### Box 8. Artificial Intelligence and Machine Learning

According to the OECD's AI Principles:

> *An AI system is a machine-based system that can, for a given set of human defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.*

That is, AI is the broad science of machines attempting to mimic human abilities, using AI systems. AI systems can then use a number of methods to implement AI, of which machine learning is one. Specifically, machine learning "*uses methods from neural networks, statistics, operations research and physics to find hidden insights in data without being explicitly programmed where to look or what to conclude*". Other AI facilitating methods include:

- Neural networks, which are a kind of machine learning that are inspired by the human brain.
- Deep learning, which uses neural networks across multiple layers to learn complex patterns in large amounts of data.
- Computer vision, which relies on pattern recognition and deep learning to identify the contents of a picture or video.
- Natural language processing, which is the ability of computers to analyse, understand and generate human language, using deep learning.

Sources: : OECD (2019[53]); Thomson, Li and Bolen (n.d.[54]); Marr (2016[55])

51. Further, the fact that businesses may not always appreciate the potential benefits and uses of consumer data at the time that they collect such data has implications for competition assessments, including but not limited to, market definition (Maggiolino and Ferrari, 2020[56]). This is discussed more in Section 4.2.

52. There also appears to be a feedback loop between the ability to collect consumer data, accelerate learning and improve algorithms, develop quality goods and services, attract more consumers, and collect even more consumer data (Gal and Rubinfeld, 2019[26]; Pecman, Johnson and Reisler, 2020[57]). As noted by the ACCC in its "Digital Platforms Inquiry" (ACCC, 2019, p. 7[58]):

> *The fundamental business model of both Google and Facebook is to attract a large number of users and build rich data sets about their users. The ubiquity of these platforms and their presence in related markets enable them to build particularly valuable data sets. This enables them to offer highly targeted or personalised advertising opportunities to advertisers.*
>
> *The advertising revenue can in turn be used to invest in the functionality and services provided, improving the consumer experience and attracting greater numbers of users to their platforms, as well as improving data gathering techniques.*

53. Of course, the use and analysis of consumer data is not costless. In particular, there are IT costs as well as staff costs associated with using and analysing consumer data. Indeed, many commentators have argued that the value in consumer data lies not in the data itself but in combining data into usable databases, and using algorithms and other analytics to glean insights (Körber, 2018[59]). In this way, Lambretch and Tucker (2017[60]) argue that it is access to skilled labour, rather than raw data (which they find is usually easy to replicate), that gives businesses in the digital economy a competitive advantage. This has implications for whether or not access to or ownership of consumer data confers market power, as discussed further in Section 4.2.2.

### *3.2.1. Incentives to share data*

54. Whether or not businesses share data also has implications for competition in relevant markets. Therefore, it is useful to consider what incentives businesses have to share their data.

55. In considering this issue, Engles (2016, p. 5[61]) notes that the incentive to share data may vary depending on the purpose for which a business is requesting the data. For example, if the data is being requested to develop a competing good or service, then the business may be less inclined to share the data. However, if the data is being requested to develop a complementary good or service, then it may be in a business' interests to share the data. Assessing the competition impacts of a requirement to share such data, however, will likely be case-specific and should consider not only the benefits from wider use of the data but also the impacts on the incentives to invest in the collection of such data. This is discussed in more detail in Sections 4.3 and 4.4.

56. In practice, many businesses have developed APIs, which facilitate data interoperability while allowing the business to retain control over who accesses their data and how they use it (see Section 5.1.1).

## 3.3. Possible consumer benefits and risks

57. Business collection and use of consumer data brings a range of potential benefits and risks for consumers.

### *3.3.1. Benefits*

58. In terms of potential benefits from businesses collecting consumer data, the UK Competition and Markets Authority (CMA) (2015[28]) identifies:

- the ability to grow sales through targeted advertising, which can also reduce search costs and provide targeted offers for consumers
- better consumer analysis, to support marketing activities or assess risk (e.g. in financial services markets)
- personalised products and services
- product improvement and development
- business process improvements
- the funding of zero-priced services.

### *3.3.2. Risks*

59. However, breaches of privacy, and the collection and use of consumer data has the potential to result in tangible and intangible consumer harms. As noted by Kemp (2019, p. 19[17]):

> *The more personal information is collected and stored, the more broadly it is disclosed, and the longer it is stored, the more likely it will be hacked, accidentally disclosed or used for and illegal purposes.*

60. One key risk is that a consumer's data are used for identity theft, which can have serious implications for the consumer concerned (Anderson, 2019[62]; Acquisti, Taylor and Wagman, 2016[15]; CMA, 2015[28]). In addition, consumers may experience data loss, unexpected or unapproved data collection, use or sharing, or nuisance contacts (CMA, 2015[28]). Even where consumers have willingly provided their information in one context, they may be at risk to the extent that businesses use that information in another context, or share the information. This is especially problematic given that a consumer's benefit from sharing or protecting personal information is largely context specific (Acquisti, Taylor and Wagman, 2016[15]). The fact that most de-identified consumer data can technically be re-identified is also potentially problematic in this context (PCAST, 2014[24]).

61. Second, businesses could use consumer data to discriminate against, manipulate, or exclude consumers from certain markets or products (CMA, 2015[28]; OECD, 2016[4]; OECD, 2018[7]). In particular, greater collection and use of personal data could facilitate personalised pricing, personalisation of the types of products that businesses show to different consumers, or the exclusion of certain consumers from certain offers. As discussed in the OECD's 2018 paper on "Personalised Pricing in the Digital Era", personalised pricing generally improves efficiency and often results in consumer gains by encouraging businesses to innovate and compete more intensively for each consumer (OECD, 2018[7]). However, in some circumstances it may result in consumer harm if implemented by businesses with substantial market power (OECD, 2018[7]). Despite this, consumers tend to view personalised pricing unfavourably, largely because they do not consider it fair. There have also been concerns about the ability of businesses to use profiling and micro-targeting to take advantage of consumers' vulnerabilities, including behavioural biases and addictions, for example (Calo, 2014[63]; Calo and Rosenblat, 2017[64]; Zuboff, 2019[39]).

62. Cohen (2013[65]) also notes the importance of privacy and freedom from surveillance to "informed and reflective" citizenship, as well as to the capacity for innovation. A loss of privacy could also reduce consumer trust in markets, which could lead to less consumer engagement, with consequent costs. Further, there may be wider social risks that arise from business use of consumer data including the potential *"manipulation of news feeds, search results, the rise of echo chambers, and, more broadly, the market for ideas"* (Ezrachi and Roberston, 2019, p. 6[49]). There have also been concerns raised about the ability of the widespread use of consumer data and online advertising to circulate propaganda and influence democratic processes (Stucke, 2018[66]). Further, if relatively few businesses hold the majority of consumer data, and are also competing for government contracts, there might be scope for businesses to be prone to government capture, which could potentially facilitate widespread surveillance by government (Stucke, 2018[66]).

## 3.4. Market failures

63. There are a number of possible market failures associated with the collection and use of consumer data including i) asymmetric information; ii) externalities; and iii) a possible lack of competition. These are discussed in more detail below.

### *3.4.1. Asymmetric information*

64. Asymmetric information can occur where there is an imbalance in information between buyers and sellers, which can potentially lead to inefficient market outcomes. In particular, if consumers cannot verify information before making a purchase, this can lead to an "adverse selection" or "lemons" problem, where higher quality goods (e.g. more privacy protective goods and services) are driven out of the market (Akerlof, 1970[67]).[2] A common regulatory response to asymmetric information is to require businesses to publish certain information to allow consumers to make more informed decisions and hence, drive effective competition. In addition, there are often protections against businesses misleading consumers under consumer protection laws (see also Section 5.2). The effectiveness of such policies as they relate to consumers' ability to engage meaningfully with privacy as an element of a good or service's quality may be relevant to competition assessments as discussed in more detail in Section 4.2.3.

### *3.4.2. Externalities and non-rivalry*

65. Consumer data are non-rivalrous (Acquisti, Taylor and Wagman, 2016[15]). This means that their use in one task does not diminish their ability to be used for another task. This can be contrasted with rivalrous goods such as oil, for example, which is exhausted once it has been extracted and consumed (OECD, 2019[12]). Some have also argued that, once shared, consumer data may be non-excludable in that business may find it difficult to exclude certain consumer data from being used by other market players (see, e.g. Acquisti, Taylor and Wagman (2016[15])). However, it is not clear that this is always the case, as discussed in more detail in Section 4.2.2.

66. In addition, as noted by Acquisti et al. (2016, p. 445[15]) *"both positive and negative externalities arise through the complex interplay of data creation and transmission"*. These positive and negative externalities relate to the fact that a consumer's data can be used to infer things about other consumers, using algorithms, machine learning and AI systems. This can allow insights to be gleaned about a consumer even where the consumer has been careful not to reveal this information. For example, if a business knows certain information about a consumer, it may be able to categorise the consumer in order to infer other information about her based on what it knows about that type of consumer more generally. The ability to combine data from multiple individuals to form a big data set capable of being able to extract useful inferences about individuals or society more broadly can have positive or negative impacts for both the individuals who contributed the data as well as society more broadly, depending on what the data set is used for. For example, if a business is using a combined data set to predict traffic or improve healthcare outcomes, this could have positive externalities. In comparison, if a business is using consumer data set to micro-target individuals and discriminate against them (where they have withheld relevant data but it has been inferred about them from others' data), then this could represent negative externalities (Gal and Rubinfeld, 2019[26]). Given these externalities, it is not surprising that Acquisti et al. (2016[15]) conclude that the economic impacts of less privacy

[2] In American slang, a "lemon" is a car that is found to be defective after it has been bought.

and more information sharing, both for consumers and society more generally, can be welfare enhancing or diminishing.

67. The existence of externalities may mean that consumer data are collected and traded at sub-optimal levels in terms of maximising welfare. For example, Choi, Jeon and Kim (2019[68]) have found that if the negative externalities associated with data collection and use outweigh the positive externalities, there will be a tendency towards data collection above the socially optimal level, even if consumers are fully informed and consumer consent is required.

### *3.4.3. Imperfect competition*

68. Other academics have argued that a lack of privacy protection in certain markets may be the result of market power in those markets. For example, Robertson (2020, p. 165[16]) notes *"consumers regularly do not get a real say in questions of privacy as part of the quality of an online product, as they are usually not able to bypass certain prevalent digital service providers"*. To the extent that anticompetitive mergers, agreements or conduct result in sub-optimal levels of privacy and data protection, there is arguably a role for competition policy and enforcement. There is also arguably a role for competition (and possibly other policy areas) in addressing demand-side factors such as behavioural barriers to switching, asymmetric information and network effects. These issues are discussed in more detail in Section 4 below.

## 4. Role of competition law enforcement

69. While businesses have collected and used consumer data for a long time, these practices have grown exponentially in recent times and the collection and use of consumer data is now core business for many firms. This means that consumer data is increasingly relevant to competition assessments. This can manifest in two key ways: i) privacy and data protection might be an aspect of quality on which businesses may compete; ii) the collection and ownership of consumer data, and access to that information, might impact competition.

70. Calls for greater consideration of privacy and data protection issues in competition assessments have increased over time. In 2014, the European Data Protection Supervisor (EDPS) advocated for a more joined up approach to data protection in its preliminary opinion on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the digital economy" (EDPS, 2014[30]). In particular, it highlighted issues associated with zero-price markets in which consumers "pay" with their data, and the impacts of privacy on consumer welfare. It argued that, in failing to consider the impacts of merging consumer data in the *Google/DoubleClick* merger (discussed further in Section 4.1.1), the European Commission (EC):

> *… neglected the longer term impact on the welfare of millions of users in the event that the combined undertaking's information generated by search (Google) and browsing (DoubleClick) were later processed for incompatible purposes. (EDPS, 2014, p. 30[30])*

71. Similarly, in 2015, the CMA published a report on the commercial use of consumer data, which looked at some of the interactions between competition and privacy outcomes, including potential demand-side barriers to better privacy outcomes (CMA, 2015[28]). These issues were also touched on in the OECD's 2016 report on "Big Data" (OECD, 2016[4]). In the same year, a joint report between the German and French competition authorities, also considered the interplay between competition law and data. While it noted

that privacy concerns are not *"within the scope of intervention of competition authorities"*, it also stated that (Bundeskartellamt and Autorité de la concurrence, 2016, pp. 22-24[69]):

> *... privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services.*

72. Privacy as an aspect of competition was also discussed in the OECD's 2018 report on "Quality considerations in the zero-price economy (OECD, 2018[6]). Further, the UK 2019 "Furman report" on "Unlocking digital competition" noted, *"the misuse of consumer data and harm to privacy is arguably an indicator of low quality caused by a lack of competition"* (Furman et al., 2019, p. 43[70]).

73. There are still few cases where issues relating to consumer data rights have been accepted or determinative, as will be discussed further below. Nonetheless, there appears to be growing acceptance that these issues may be relevant to competition assessments (OECD, 2016[4]; OECD, 2018[6]; OECD, 2018[5]; Robertson, 2020[16]; Kemp, 2019[17]). This section considers the role for competition enforcement in relation to consumer data rights. First, it considers potential theories of harm. Next, it considers analytical issues, such as market definition, barriers to entry, consumer attitudes towards privacy, how to assess levels of privacy and data protection, and potential efficiencies. It then considers potential remedies and the potential role of the essential facilities doctrine.

## 4.1. Relevant theories of harm

74. There are a number of potential theories of harm associated with consumer data and consumer data rights, as outlined below. These encompass merger, abuse of dominance and cartel cases.

### *4.1.1. Mergers*

75. Mergers between businesses that use consumer data could potentially harm competition in two ways: i) by reducing the quality of data protection and privacy on offer in the relevant market, or ii) by raising barriers to entry or raising rivals' costs through the merging of consumer data.

76. Concerns about mergers reducing competition in respect of the collection and use of consumer data might be especially relevant in zero-price markets where competition is largely on elements of quality rather than price (OECD, 2018[6]). Further, Gilbert and Pepper (2015, p. 5[52]) suggest that: "*The removal of an important "maverick" that has developed innovative data-protection and control systems could potentially raise competition issues by reducing innovation in data privacy, even if the merging parties were not otherwise close competitors.*" Condorelli and Padilla (2019[71]) also put forward a "privacy policy tying" envelopment strategy which could potentially be used to increase the amount of consumer data collected as part of a conglomerate merger. Under this theory, a dominant firm would obtain broad consumer consent from its users, allowing it to use this consent in new markets that it enters via a merger where there are overlapping consumers in both markets. This theory of harm is discussed in more detail in the OECD's background note on "Conglomerate effects of mergers" (OECD, 2020[10]).

77. There seems to be growing acceptance that privacy may be relevant to merger assessments to the extent that it is a dimension of quality that consumers value, and hence on which businesses compete. That said, there do not appear to be any mergers that

competition authorities have blocked on the basis of such concerns alone, as discussed below.

78. Mergers could also potentially have an anticompetitive impact where the merging of consumer data has the potential to raise barriers to entry or raise rivals' costs. In such cases, a potential remedy could be to require the merged party to grant access to its merged data set. In practice, a number of mergers have been blocked, or allowed with conditions, due to concerns about the merged party's consumer data assets having an anticompetitive effect in the relevant market. Some examples are discussed below.

79. Relatedly, certain mergers may be motivated by a desire to access a competitor's data set. This could potentially be a motivation for a number of so-called "killer acquisitions" and "nascent acquisitions", for example. Issues associated with killer and nascent acquisitions, including but not limited to merger notification thresholds, will be addressed in a separate roundtable scheduled for June 2020 on "Start-ups, killer acquisitions and merger control" (OECD, 2020[9]).

### *Relevant cases*

80. In its assessment of the *Google/DoubleClick* merger in 2008, the EC deferred privacy considerations to data protection law, following the precedent set by *Asnef-Equifax* (see next section). *Google/DoubleClick* involved a merger between two parties with the ability to collect and use substantial quantities of consumer data: Google through its Internet search services, and DoubleClick through its "ad serving" services. While the EC discussed how these businesses used consumer data, it relied on data protection legislation (rather than competition law) to uphold privacy, noting that (2008, p. 98[72]):

> *Irrespective of the approval of the merger, the new entity is obliged in its day to day business to respect the fundamental rights recognised by all relevant instruments to its users, namely but not limited to privacy and data protection.*

81. In the United States, the FTC took a similar position in its assessment of the *Google/DoubleClick* merger. While it did not consider that antitrust can nor should consider privacy implications, it nonetheless found that the merger would not harm non-price aspects of competition (2007, pp. 1-2[73]):

> *Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry. That said, we investigated the possibility that this transaction could adversely affect non-price attributes of competition, such as consumer privacy. We have concluded that the evidence does not support a conclusion that it would do so. We have therefore concluded that privacy considerations, as such, do not provide a basis to challenge this transaction.*

82. Even in her dissenting statement on the *Google/DoubleClick* merger, Commissioner Pamela Jones Harbour, while raising potential privacy concerns, ultimately agreed that *"a more comprehensive approach to privacy is preferable"* (Jones Harbour, 2007[74]). That is, she was of the view that privacy protections should apply across the economy rather than be implemented in respect of specific competition cases. Notwithstanding this, a merger could arguably reduce the level of data protection offered in the relevant market even where data protection legislation sets minimum standards since competition could arguably raise levels of data protection above such minimum standards.

83. These decisions have since been criticised, among other things, for not taking into consideration the impact on third-party tracking (Ezrachi and Roberston, 2019[49]; Binns

and Biettib, 2019[50]). In this respect, Ezrachi and Robertson (2019, p. 11[49]) question whether the *Google/DoubleClick* merger reflected "*an underestimation of the true (aggregated) data advantage*".

84. The EC maintained the legal separation between competition and consumer data issues in its consideration of the *TomTom/TeleAtlas* merger involving a vertical merger between a provider of navigation services and a provider of digital maps. In particular, the decision did not consider impacts on privacy and personal data protection (EC, 2008[75]). Further, in a number of decisions that followed, the EC appeared to rely on the European data protection laws to limit the extent to which the relevant mergers could lead to a reduction in privacy, through greater collection, aggregation or use of consumer data.

85. In *Telefonica UK/Vodafone UK/Everything Everywhere* in 2012, the EC considered the competitive impacts of a joint venture to offer various mobile commerce services in the United Kingdom (European Commission, 2012[76]). In doing so, the EC noted that the joint venture would be restricted by data protection laws that require consumers to opt-in to the proposed forms of data collection and use (Zanfir-Fortuna and Ianc, 2019[77]).

86. Also in 2012, the FTC and the UK (former) Office of Fair Trading allowed the *Facebook/Instagram* merger, with neither competition authority seemingly considering whether the merger might impact on privacy and data protection (OFT, 2012[78]; FTC, 2012[79]).

87. In 2014, the EC (2014[80]) allowed the *Facebook/WhatsApp* merger, a merger between a social media network and a communications app, which both collected and used varying amounts of consumer data. In reviewing the merger, the EC considered the ability for the merged entity to combine consumer data from Facebook and WhatsApp. It accepted the submission from the merger parties that this would be technically difficult, but in any case, noted that the competitive impact of this would be limited given the significant overlap of users. Further, it deferred privacy considerations to data protection laws, stating that (2014, p. 29[80]):

> *Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.*

88. In discussing the decision, staff from the EC noted that privacy could be a non-price parameter of competition and that an increasing number of consumers value privacy. However, they also noted that the majority of consumer communications apps do not compete on privacy, and hence, they concluded that competition on privacy was not a relevant consideration in the *Facebook/WhatsApp* merger (Ocello, Sjödin and Subočs, 2015[81]). Differences in the level of privacy offered were also seen by the EC as indicative of Facebook and WhatsApp operating in different markets. Lynskey (2018[82]) subsequently criticised the EC for this "logical fallacy" which overlooked the possibility that WhatsApp had differentiated itself in respect of data protection.

89. As a follow-up to the *Facebook/WhatsApp* merger, in 2017, the EC fined Facebook EUR 110 million for providing incorrect or misleading information to the EC in support of its 2014 assessment (European Commission, 2017[83]). Namely, the EC became aware that Facebook knew of a possible technical solution to automatically match Facebook and WhatsApp user identities at the time of the merger. However, the EC noted that this would not change its 2014 assessment, especially as it had considered this possibility in clearing the merger.

90. The *Facebook/WhatsApp* merger was also cleared in the United States, but in doing so, the FTC wrote to both parties to highlight their obligations to protect consumer privacy (Rich, 2014[84]; FTC, 2014[85]). In particular, the letter noted the need for businesses to gain consumer consent before making changes to the collection and use of consumer data. It also noted that businesses must not misrepresent the extent to which they maintain the privacy or security of user data, and recommended that businesses allow consumers to opt out of any future changes to how data is used.

91. As a general point, Körber (2018, p. 14[59]) notes that integrating separate databases "*is a complex, time consuming and cost intensive endeavour*". Notwithstanding this, Lynskey (2018[82]) suggests that the starting assumption should be that the merging parties can and will merge their data sets. This appears to be the approach taken by the EC and the FTC in clearing the *Facebook/WhatsApp* merger.

92. In the same year, the FTC also cleared the *Google/Nest Labs* merger, which brought Nest, a smart home device manufacturer with the potential to collect masses of consumer data, under the same umbrella as Google (FTC, 2014[86]). It is not clear whether the FTC considered the potential impact on privacy in clearing this merger.

93. Also in 2014, consumer data as a barrier to entry was one of the factors considered in the *Bazaarvoice/PowerReviews* merger, which involved a horizontal merger between two rating and review platforms (United States v. Bazaarvoice, 2014[87]; Ohlhausen, 2019[88]). The US Department of Justice (DoJ) challenged the merger due to broader horizontal concerns (Ohlhausen, 2019[88]).

94. In 2016, the EC allowed the *Microsoft/LinkedIn* merger, noting that while privacy is a significant factor of quality in the market for professional social networks, the European data protection laws will limit the extent to which the merged entity can combine data from the two companies (2016, p. 55[89]):

> *Microsoft is subject to European data protection laws which limit its ability to undertake any treatment of LinkedIn full data. While, today's LinkedIn's privacy policy allows it to share the personal data it collects, processes, stores and uses with its controlling companies, this is only for the purposes described in the privacy policy itself … [T]he newly adopted General Data Protection Regulation … may further limit Microsoft's ability to undertake any treatment of LinkedIn full data by strengthening the existing rights and empowering individuals with more control over their personal data (i.e. easier access to personal data; right to data portability, etc.).*

95. In its press release on the approval of the *Microsoft/LinkedIn* merger, the EC clarified its position regarding the consideration of privacy issues in merger cases (EC, 2016[90]):

> *Privacy related concerns as such do not fall within the scope of EU competition law but can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor.*

96. Aside from the potential impact on privacy, the EC has been criticised for not taking enough consideration of the impact of the *Microsoft/LinkedIn* merger on third-party tracking (Binns and Biettib, 2019[50]). In particular, Ezrachi and Robertson (2019, p. 9[49]) found that the *Microsoft/LinkedIn* merger "*significantly increased the scope and range of data acquired through third-party tracking*" for the merged entity. Moreover, Ezrachi and Robertson (2019, pp. 8-9[49]) note:

*Wide ranging third-party tracking, controlled by a single company, can reinforce the data advantage that certain tech companies are already benefitting from.*

97. Also in 2016, the EC (2016[91]) relied on the right to data portability under the GDPR to protect consumers against lock-in effects with respect to a Joint Venture between subsidiaries of Google and Sanofi to offer services for the management and treatment of diabetes, including data collection, processing and analysis. Arguably, competition remedies could have been used in this case to more directly and expediently address potential problems of lock-in – see Section 4.3.

98. In considering the *Apple/Shazam* merger in 2018, the EC looked at the role of consumer data in the relevant markets (EC, 2018[92]). It noted that the parties gathered a range of data and noted the important and growing role of user data in the music industry. It then considered the ability of Apple to use its user data to strengthen Shazam's position in respect of online advertising for music enthusiasts. However, it considered that this would not significantly impede competition given there are a number of larger market players that could compete in this regard. It also considered whether Shazam's user data could be considered an important input for providers of digital music streaming apps. It ultimately considered that even if the merged entity were to deny access to Shazam user data to Apple's competitors, this would be unlikely to raise barriers to entry and thus impede competition.

99. As this history shows, there appears to be a growing realisation that companies can compete on the level of data protection provided as an aspect of the quality of their offer. In addition, there has been some consideration of the impacts of merger parties combining their consumer data sets on competition. It appears that competition authorities are increasingly considering these issues in merger assessments. However, a merger is yet to be challenged on the basis that it would reduce the level of data protection in the relevant market. Further, in many cases, competition authorities have relied on the need for consumer consent for the collection and use of consumer data, to limit the ability of the merged entity to merge its consumer data sets. That is, they have relied on data protection laws to constrain the ability of merging companies from using consumer data or degrading data protection in an anticompetitive way. Whether this is a reasonable assumption is discussed in more detail in Section 4.2.3.

### *4.1.2. Abuse of dominance*

100. In theory, a dominant firm could abuse its dominance by lowering the level of privacy and data protection it offers to consumers (Kemp, 2019[17]; Ezrachi and Roberston, 2019[49]). This could arguably constitute an exploitative abuse in some jurisdictions. For example, Stucke (2018, pp. 285-286[66]) argues: "*A data-opolist, to the extent its business model depends on harvesting and exploiting personal data, has the incentive to reduce its privacy protection below competitive levels and collect personal data above competitive levels.*" Further, it has been argued that in jurisdictions that are able to prosecute against excessive prices by dominant businesses, the same laws could be used to guard against unfair data collection by a dominant firm (Ezrachi and Roberston, 2019[49]). However, in practice, there are few examples of these types of cases, as discussed below.

101. In addition to the exploitative theory of harm discussed above, there is potential for an exclusionary abuse of dominance theory of harm. In particular, foreclosure could potentially occur where a dominant firm engages in exclusionary conduct that restricts competitors' access to consumer data. Alternatively, where a dominant firm has exclusive access to consumer data, it could attempt to raise rivals' costs or barriers to entry by engaging in tying or bundling.

*Relevant cases*

102. In respect of exclusionary conduct in the energy sector, both the French and UK competition authorities have required retail energy businesses to make their customers' energy data available to competitors (via Ofgem in the case of the United Kingdom) to facilitate greater competition (CMA, 2016[93]; Autorité de la concurrence, 2014[94]). To address privacy concerns in these cases, consumers were given the opportunity to opt-out of sharing their data. The Italian competition authority similarly found that the exclusive control of customer lists by two regulated energy companies could foreclose competition in the provision of liberalised energy services (Maggiolino and Ferrari, 2020[56]).

103. In comparison, there appears to be only one exploitative case taken to date involving consumer data. In 2019, Germany's competition authority, the Bundeskartellamt, found that Facebook had abused its dominant position in the social media market in respect of the collection of "off Facebook" data (see Box 9). It is the first decision that has argued a theory of harm relating to a reduction in privacy as an abuse of dominance.

### Box 9. Bundeskartellamt case against Facebook

In March 2016, the Bundeskartellamt launched an abuse of dominance investigation of Facebook in respect of its data practices. In February 2019, it found that Facebook had abused its dominant position in the social media market in respect of the collection of "off Facebook" data (i.e. data from unrelated third parties). In particular, in using Facebook's services, users had to agree to Facebook collecting their data both on Facebook, and across an extensive range of third party websites and apps.

The Bundeskartellamt found that Facebook was dominant in the social media market in Germany. It also found that Facebook had not gained meaningful consent from users in respect of its data tracking practices, and the merging of this data to users' Facebook profiles. In assessing the data practices of Facebook, the Bundeskartellamt applied the standards in Europe's GDPR and found Facebook's practices lacking, which it found amounted to an abuse of dominance. It argued that Facebook's dominant market position essentially put consumers in a "take-it-or-leave-it" position and it found that Facebook's data practices served to entrench Facebook's dominant position. Throughout the investigation, the Bundeskartellamt maintained regular contact with data protection authorities. Its decision required Facebook to amend its data collection and processing practices within 12 months.

Facebook appealed the decision to the Higher Regional Court in Dusseldorf, who suspended the order in August 2019. In particular, it did not accept that a possible violation of privacy rules would automatically trigger a violation of antitrust rules in the case of a dominant company. In addition, the court was of the opinion that users decide autonomously whether they agree with Facebook's terms and conditions when signing up for the service. It further found that Facebook's data collection was not exploitative since consumers could continue to make the same data available to other companies. Moreover, it found that the Bundeskartellamt did not demonstrate how Facebook's data practices damaged competition. The suspension of the order relieved Facebook from implementing the Bundeskartellamt's decision. The Bundeskartellamt has appealed the suspension to the Federal Court of Justice and the appeal is ongoing.

Sources: Bundeskartellamt (2019[95]): Bundeskartellamt (2019[96]); *Facebook/Bunderskartellamt*, Decision of the Higher Regional Court of Düsseldorf in interim proceedings, 26 August 2019, Case Vi-Kart 1/19 (V); CPI (2019[97]); Colangelo and Maggiolino (2018[98]); Këllezi (2019[99]).

104. In taking the *Facebook* case, a key challenge for the Bundeskartellamt was to show that Facebook had misused its market power in forcing users to accept excessive data collection practices. In doing so, it used the GDPR as a normative standard. Ultimately, as outlined in Box 9, the Higher Regional Court in Duesseldorf did not accept this approach. The Bundeskartellamt has also been criticised for not providing any counterfactual analysis, and for failing to show that consumers do value privacy in the market for social networks in Germany (Këllezi, 2019[99]). In addition, it was criticised for not showing the anticompetitive effects of Facebook's conduct (Këllezi, 2019[99]). However, this decision has been appealed and the case is ongoing.

105. More broadly, however, demand-side factors could make cases like this particularly difficult, as discussed in more detail in Section 4.2.3. In particular, the fact that so few consumers engage with and understand privacy notices, whether from a dominant business or otherwise, is a key challenge for any case trying to prove that a dominant business' data collection practices are excessive (Höppner, 2019[100]; Colangelo and Maggiolino, 2018[98]; Chirita, 2018[101]).

### *4.1.3. Cartels and collusion*

106. While no cases appear to have been introduced to date, collusion that agrees on the level of privacy offered to consumers could potentially constitute a cartel infringement as with any other agreement on quality, output or price. Similarly, an agreement to provide services at zero-price on the basis that this will maximise the collection and use of consumer data, could potentially raise competition concerns (OECD, 2018[6]).

107. In addition, sharing of data between competitors can sometimes raise competition concerns. However, it is less clear that sharing consumer data between competitors, in and of itself, could facilitate collusion. In particular, if the data does not include information about price, quality, innovation, or choice, it is not obvious that sharing consumer data could facilitate collusion. In practice, relevant competition cases have tended to allow sharing of consumer data as it has usually been found to foster competition.

#### *Relevant cases*

108. The *Asnef-Equifax* case of 2006 is often cited as one of the first cases in which matters of privacy were considered by the European Court of Justice but ultimately deferred to data protection legislation, rather than competition law. *Asnef-Equifax* involved an agreement between competing financial institutions to create a register to share consumer solvency and credit information to evaluate credit and lending risks (European Court of Justice, 2006[102]). In considering the potentially anti-competitive agreement, which facilitated the sharing of personal data, the European Court of Justice (2006, p. 20[102]) noted:

> *... any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection.*

109. It ultimately cleared the agreement on the basis that it would foster competition in the provision of financial services that require such information.

110. In 2019, the Brazilian government enacted legislation to develop the "Personal Credit Report", which was implemented on an opt-out basis to cover all consumers by default (Banco Central do Brasil, 2019[103]). This followed a 2016 decision by Brazil's competition authority (CADE) to allow a joint venture between Banco do Brasil, Bradesco, Caixa Econômica, Itaú and Santander, which created a new credit bureau. In particular, it considered that the benefits from a consolidated solvency register would outweigh the

potential impacts on competition (CADE, 2016[104]). Potential competition impacts were addressed through a Merger Control Agreement, which guaranteed non-discrimination for competing credit bureaus accessing credit information and mechanisms of corporate governance in order to avoid information exchange between the associated banks through the joint venture.

## 4.2. Analytical challenges

111. As some of the above cases have highlighted, there are a number of analytical challenges involved in cases involving consumer data. These include challenges associated with market definition, barriers to entry, demand-side factors, measuring data protection, and assessing pro-competitive efficiencies. These issues are discussed below.

### *4.2.1. Market definition*

112. There has been discussion in the competition literature about whether in some cases it might be appropriate to define a "market for data" (Costa-Cabral and Lynskey, 2017[105]). For example, Jones Harbour and Koslov (2010, p. 773[106]) note that:

> *Data market definition would reflect the distinction between data collection at one point in time and expanded data usage at some later date … Internet-based firms often derive great value from user data … and this data often has important competitive consequences. In contrast, product market definitions based only on a snapshot of current data usage may not accurately capture this aspect of competition.*

113. Similarly, Forrest (2019[107]) has argued that a firm's data and its algorithmic ability to analyse such data are themselves products. In this way, "*the potential commoditization of a data set works as a proxy to define a competitive universe*" (Forrest, 2019, p. 12[107]). In contrast, Körber (2018, p. 2[59]) states "*there is no more a single* "*market for data" than there is a single "market for raw materials"*".

114. Alternatively, Jones Harbour and Koslov (2010[106]) note that the competitive impacts in data-intensive markets could be assessed by considering barriers to entry. They note a number of mergers in which competition authorities considered the competitive effects of merging otherwise competing data sets. These spanned data relating to "estimatics", financial data, health data and entertainment data (2010[106]). Given there is some substitutability between assessing competition impacts via market definition or an assessment of barriers to entry, perhaps an assessment of barriers to entry is a less controversial approach. This is discussed below.

115. In addition, given the number of two-sided and multi-sided markets that rely on consumer data, complexities relating to market definition in these types of markets may also be relevant. For more on this topic, see the OECD's 2018 report on "Rethinking Antitrust Tools for Multi-sided Platforms" (OECD, 2018[108]).

### *4.2.2. Barriers to entry*

116. Several aspects of digital markets tend to suggest that barriers to entry could be high in markets involving consumer data. In particular, increasing returns to scale, economies of scope and network effects are often present in markets involving consumer data (Kemp, 2019[17]). Where these require a business to incur substantial sunk costs to enter the relevant market, they could represent barriers to entry. Rubinfeld and Gal (2017[37]) have undertaken an in-depth analysis of the data supply chain to identify possible

barriers to entry associated with the collection, storage, synthesis and analysis, and use of data. These are summarised in Table 1 and discussed in more detail below.

**Table 1. Barriers to entry in the data supply chain**

| | Technical barriers | Legal Barriers | Behavioural barriers |
|---|---|---|---|
| Collection | • Uniqueness of the data, or access to it<br>• Supply side: economies of scale, scope, learning by doing, speed<br>• Demand side: network effects and two-sided markets | • Data protection and privacy laws<br>• Data ownership | • Exclusivity agreements<br>• Access prices and conditions<br>• Disabling data collecting software |
| Storage | • Storage costs | • Data protection and privacy laws | • Lock-in and switching costs |
| Synthesis and analysis | • Lack of interoperability (including a lack of standardisation)<br>• Analytical tools | | |
| Use | • Inability to locate and reach relevant consumers<br>• Lack of interoperability (including a lack of standardisation) | • Data protection and privacy laws<br>• Anti-discrimination laws | • Contractual limitations |

Source: Rubinfeld and Gal (2017[37]); Gal and Rubinfeld (2019[26]); CMA (2016[93])

117. In respect of the collection of data, Rubinfeld and Gal (2017[37]) found that if a business has unique access to unique data, this might be difficult to recreate without incurring substantial sunk costs. As an example, gaining access to the posts and reactions of consumers on a dominant social media network might be difficult to recreate. As noted by Maggiolino and Ferrari (2020, p. 41[56]):

> *… an empirical analysis of the factual circumstances on a case-by-case basis should always be carried out to assess whether the same data (i.e. the data responding to the same needs) could be obtained elsewhere on the market.*

118. In this respect, the analysis should look at the business' access to both first party and third-party data.

119. Rubinfeld and Gal (2017[37]) also found that technological supply-side barriers could arise where incumbents have achieved economies of scale or scope, or "learning by doing". The largely fixed and sunk costs involved in collecting data at high velocity might also raise barriers to entry (Pecman, Johnson and Reisler, 2020[57]). A key empirical issue in relation to this is to assess the point at which diseconomies of scale and scope set in. For example, work by Chiou and Tucker (2017[109]) suggests that, at least for online search engines, access to longer periods of historical data does not necessarily confer a significant advantage. Körber (2018[59]) similarly finds that data is subject to declining marginal returns, in that each additional piece of data yields less information. Conversely, however, others have argued that data could actually have increasing returns to scale (Gal and Aviv, 2020[110]). In this respect, the ability of a potential rival to recreate an incumbent's dataset in terms of the volume, velocity and variety of the data is of key importance, as discussed in Section 2.2.3.

120. There may also be demand-side barriers to entry with respect to the collection of data; for example, where network effects are present. The presence of two-sided markets and the fact that to collect some types of data requires entry into a related market (what Rubinfeld and Gal (2017[37]) call two-level entry), can also increase the sunk costs required to enter the relevant market. In addition, legal barriers such as data protection and privacy

laws can raise entry barriers. Behavioural barriers such as exclusivity agreements and discriminatory access prices or conditions may also be relevant in some markets involving data. Similarly, any tying or bundling in relation to the collection of consumer data may warrant further analysis to assess its effect on competition.

121. With respect to storage, Rubinfeld and Gal (2017[37]) note the costs of storage are declining, making this more unlikely to be a barrier to entry than it may have been previously (especially where such costs are not sunk). They also cite legal barriers, such as legal limitations on where someone's personal data can (physically) be held. In addition, they note that high switching costs with respect to storage could lead to lock-in. Regarding data synthesis and analysis, they note a number of potential technical barriers including limits to data interoperability, and the costs associated with developing analytical tools. Last, they consider potential barriers associated with the use of data, noting difficulties in locating relevant consumers, contractual limitations on the ability to use data in different ways, as well as legal barriers to how data can be used.

122. Various competition agencies have found that an incumbent's access to consumer data may raise barriers to entry in a number of digital platform markets. As noted by the Bundeskartellamt (2019[95]) in its *Facebook* decision:

> *The high competitive relevance of the data base to a supplier of social networks will, however, create an additional barrier to market entry …*

123. The ACCC, in its "Digital Platforms Inquiry" found (ACCC, 2019, p. 11[58]):

> *The breadth and depth of user data collected by the incumbent digital platforms provides them with a strong competitive advantage, creating barriers to rivals entering and expanding in relevant markets, and allowing the incumbent digital platforms to expand into adjacent markets…*

124. The ACCC's conclusion highlights the importance of considering all sources of data that a business has access to, and of assessing whether such access is unique or replicable. In addition, the importance of consumer data to improving the underlying good or service and attracting more consumers (i.e. the "feedback loop") is also important. In this respect, Colangelo and Maggiolino (2018, p. 2[98]) note:

> *… the collection and aggregation of data, including personal data, by dominant firms entrenches their dominant positions … the more data a firm gathers and analyzes, the better its products, the more users it attracts, the more data it collects and processes, and so on.*

125. Acquisti et al. (2016, p. 444[15]) further note:

> *… a few "gatekeeper" firms are in a position to control the tracking and linking of those behaviours across platforms, online services, and sites—for billions of users. As a result, chronicles of peoples' actions, desires, interests, and mere intentions are collected by third parties, often without individuals' knowledge or explicit consent, with a scope, breadth, and detail that are arguably without precedent in human history.*

126. In summary, as noted above, the assessment of whether the merging of consumer data sets, or efforts to restrict access to consumer data, will likely raise barriers to entry has to be undertaken on the specific facts of the case. In assessing barriers to entry, factors outlined in Table 1, to the extent that these represent sunk costs, may be relevant factors to consider.

### *4.2.3. Consumer attitudes towards privacy*

127. A key issue in understanding competitive dynamics in markets involving consumer data is to understand consumer attitudes and behaviours in respect of privacy and data protection in the relevant market (Manne and Sperry, 2015[111]). At a general level, while attitudes to privacy vary between individuals depending on a number of factors, numerous surveys have shown that consumers do value privacy and are increasingly concerned about their privacy online (Cisco, 2019[112]; Auxier et al., 2019[113]; RSA, 2019[114]). However, in the context of a competition assessment, complexities on the demand side of the market can make it difficult to understand the importance of privacy and data protection to consumers in the specific markets under investigation.

128. First, consumer attitudes regarding privacy are *"subjective and idiosyncratic"* (Acquisti, Taylor and Wagman, 2016, p. 446[15]). In particular, consumers tend to have heterogeneous preferences when it comes to privacy (Walters, Zeller and Trakman, 2018[115]). Further, even for the same individual, the decision about whether to share or withhold personal information will depend on the context in which the information is requested (Acquisti, Taylor and Wagman, 2016[15]). However, in practice, this is often the case for many aspects of a business' competitive offer, so it is something that competition agencies have much experience with.

129. Behavioural biases may also lead consumers to overshare their data or agree to low levels of privacy. One issue is that privacy trade-offs are intertemporal in that sharing data will likely to bring an immediate (and more certain) benefit, as compared to the risks of an uncertain cost at some unknown future date (Acquisti, Taylor and Wagman, 2016[15]). This can be particularly problematic given that consumers tend to be myopic and subject to time inconsistent preferences (Choi, Jeon and Kim, 2019[68]). The way in which privacy options are presented can also lead to greater sharing of data given consumers have a tendency to stick with default privacy settings due to the status quo bias (Costa-Cabral and Lynskey, 2017[105]). In addition, consumers may underappreciate privacy in zero-price markets (and over-appreciate the benefits of the free good or service) due to the "free effect" (OECD, 2018[6]).

130. Commentators have also raised concerns about consumers' lack of bargaining power in respect of privacy notices, which tend to be provided on a "take it or leave it" basis (Hull, 2014[116]; Costa-Cabral and Lynskey, 2017[105]). Such concerns may well reflect a lack of effective competition in the market. Alternatively, the inability of consumers to engage with privacy policies, and behavioural biases limiting consumers' ability to meaningfully engage with privacy policies may result in consumers agreeing to policies that they do not actually agree with. Such outcomes could undermine the effectiveness of data protection laws that rely predominately on consumer consent to ensure good data protection outcomes. In this respect, there have been serious concerns raised about consumers' ability to understand and act on privacy notices (Hoofnagle and Whittington, 2014[117]). The ACCC, in its *"Digital Platforms Inquiry"* (ACCC, 2019, p. 2[58]), found:

> *... few consumers are fully informed of, fully understand, or effectively control, the scope of data collected and the bargain they are entering into with digital platforms when they sign up for, or use, their services.*

131. For example, surveys carried out by the ACCC showed that 36% of consumers (wrongly) believe that the mere existence of a privacy policy means that businesses will not share personal information with third parties (ACCC, 2019[58]).

132. These issues can manifest in the so-called "privacy paradox", where, despite expressing concerns about privacy, and rating it as important, consumers do not appear to make decisions with privacy in mind (Norberg, Horne and Horne, 2007[118]; Kokolakis,

2017[119]; OECD, 2018[6]). For example, 79% of Americans in 2019 were concerned about the way their data was used by companies and 81% believed the potential risks associated with data collection outweighed the benefits (Auxier et al., 2019[113]). Alternatively, it may be that while consumers do value privacy, they value it less than other product characteristics, such as lower prices and greater functionality. Indeed, this was the finding of an experiment by Preibusch, Kübler and Beresford (2013[120]) in which an overwhelming majority chose to make an online DVD purchase from a less privacy-friendly company when it offered the product for a lower price. Even when privacy was the only element that varied, the choice of retailer appeared to be quite random. This may be why so few businesses have differentiated themselves on privacy alone (OECD, 2018[5]). It might also explain why more privacy-friendly businesses have not achieved substantial market shares in their respective markets (for example, DuckDuckGo, an Internet search engine that differentiates itself by not collecting any consumer data is yet to obtain any substantial market share).

133. Moreover, the above issues may preclude the possibility of competition on privacy even if consumers valued competition on such a parameter. As noted by the CMA (2015[28]), consumers should theoretically be able to discipline businesses over their collection and use of consumer data. That is, if consumers are not happy with the way a business uses their data, they should be able to switch. However, if consumers do not understand what data a business collects, how it uses data, and the value of the data, they may not be in a position to make decisions with privacy in mind. Hence, businesses may have limited incentives to compete on privacy (Farrell, 2012[121]; Lynskey, 2018[82]). This may be reinforced where there is a lack of competition in the relevant market and consumers do not have other viable options (Costa-Cabral and Lynskey, 2017[105]; Lynskey, 2018[82]). Taken together, these issues can make it difficult to understand in what circumstances and markets consumers actually understand and value privacy, both in theory and in practice. They may also undermine the effectiveness of consent-based models of data protection, some of which competition agencies have relied on to promote good outcomes in respect of data protection where a merger or market power may have otherwise undermined such outcomes.

134. To help understand consumer views on privacy, competition agencies may consider undertaking consumer surveys as part of the assessment of competition cases where privacy might be a relevant aspect of competition on quality. For example, in assessing the competitive impacts of a merger, it might be useful to understand whether any apparent differences in the privacy offered by the merging parties are important to consumers. In comparison, for an abuse of dominance case, it might be useful to use consumer surveys to understand whether consumers are satisfied with the level of privacy offered, and if not, why. Of course, in using this evidence, competition agencies need to be mindful that stated preferences tend to be higher than revealed preferences; an effect that seems consistent with the privacy paradox. However, given competition authorities are less interested in quantifying the exact magnitude of how much consumers value privacy and, rather, identifying whether a sufficient proportion of consumers value privacy, these limitations may be less important in practice. Surveys also have the advantage of being able to be tailored to the specific market. This is important given that privacy views are context specific and may change over time along with consumer awareness of business practices (Gilbert and Pepper, 2015[52]).

135. Consumer responses to changes (or even potential changes) to the level of privacy afforded by businesses in the relevant market may also be useful sources of evidence on the importance of privacy to consumers in that market. For example, in considering the *Facebook/WhatsApp* merger, the EC (2014[80]) cited the "thousands" of users that had downloaded different messaging platforms (in particular, Telegram) and the high number

of German users that switched from WhatsApp to Threema, after the announcement of Facebook's acquisition of WhatsApp. It noted that this switching away from WhatsApp to more privacy-friendly apps reflected the value that at least some consumers placed on privacy in this market. Consumer reactions to privacy scandals, such as the Facebook-Cambridge Analytica scandal, may also be informative where relevant examples exist.

### *4.2.4. How to assess competition on data protection*

136. In assessing a merger between two parties that appear to compete on privacy, it may be useful to understand how the privacy practices of each party compare, and how important these differences are for competition. Similarly, for an abuse of dominance case relating to a reduction in privacy or excessive collection of consumer data, it will be important to assess the dominant business' privacy and data protection practices.

137. One key challenge in an abuse of dominance case of this type would be to determine "*where legitimate data collection ends and excessive data collection starts*" (Robertson, 2020, p. 173[16]). Put differently, in the absence of effective competition, it is difficult to know what the competitive level of consumer data sharing, and privacy more generally, would be (Colangelo and Maggiolino, 2018[98]).

138. Where a competition authority has the ability to take an exploitative abuse of dominance case, Robertson (2020[16]) suggests that the principles of proportionality, equity, indispensability of a trading condition, and the parties' bargaining power, are relevant considerations in trying to prove the level of data being requested is unfair. Similarly, Colangelo and Maggiolino (2018, p. 21[98]) argue that the concept of unfairness captures clauses that that are "*unjustifiably unrelated to the purpose of the contract, unnecessarily limiting the freedom of the parties, disproportionate, unilaterally imposed or seriously opaque*". These criteria draw on the judgements of the European Court of Justice and the EC in respect of *Tetra Pak II*, *Duales System Deutschland (DSD)*, *United Brands*, and *Michelin II*. These factors will be important in determining whether the practices of the dominant business are "abusive".

139. In addition, the eight privacy principles set out in the OECD's "Privacy Guidelines" (see Box 2) may offer some guidance in how to assess the quality of privacy offered by the various market players, whether in respect of a merger or abuse of dominance case (OECD, 2013[11]). Building on these key principles, and the approaches proposed by Esayas (2018[122]) and Waehrer (2016[123]), the quality of privacy could potentially be assessed in each of the following categories:

- **Collection minimisation**: What data is collected – does the business apply data minimisation (i.e. is it the minimum required to provide the good or service)? This could be ascertained through requests to the relevant business(es) and expert opinion.
- **Use minimisation**: What is the data used for, for how long is it stored, and who is it shared with? Again, competition agencies could assess this through business requests for information, and expert advice.
- **Transparency**: What information is provided to the user in terms of data collection and use and how is it provided? Privacy policies and other related disclosures could be assessed for readability and ease of understanding.
- **User control**: Can users easily access, modify, delete and port their data; what choices does the user have? Expert assessment could assist in determining this.

- **Security and privacy by design**: What security measures are in place to protect the data from unauthorized access, accidental loss, destruction or damage; does the business use privacy enhancing technologies (PETs) such as end-to-end encryption, pseudonymisation and anonymization? Expert advice might be required to assess this, facilitated by business responses to information requests.
- **Privacy by default**: Does the business implement privacy features by default? Again, expert advice might be required to assess this, facilitated by business responses to information requests.

140. There are a number of sources of evidence that could support such an assessment. In considering mergers, for example, many competition authorities send questionnaires to the merging parties and in some cases, to their competitors. Among other things, the survey could include questions to ascertain whether privacy is an important aspect of competition in the relevant market, and whether it something that consumers value. For example, in its consideration of the *Microsoft/LinkedIn* merger in 2016, the EC undertook a questionnaire of social network business to, among other things, better understand whether privacy is an important driver of competition and consumer choice in this market (European Commission, 2016[89]).

141. In mergers, documents proving that businesses track the privacy policies of other companies might be indicative of competition in respect of privacy, especially if businesses respond to competitors changing their privacy policies (except where this is to comply with changes to regulatory requirements) (Waehrer, 2016[123]). For example, Jones Harbour and Koslov (2010[106]) note that in response to Google stating that it would shorten the time that it would keep consumer data, Microsoft reduced the time it kept data to six months, and then Yahoo! reduced this to three months. In addition, internal assessments of consumer reactions to changes in the level of privacy might suggest that this is an important aspect of competition in the relevant market, whether in relation to a merger or an abuse of dominance case.

142. For abuse of dominance cases, evidence of how the dominant business' privacy practices have changed over time in response to different levels of competition in the market may also be useful evidence. For example, Srinivasan (2019[124]) argues that recent degradations in privacy on social media networks are due to high levels of market power leaving consumers no alternative option (at least none with a pre-installed user base, reflecting the importance of network effects in these markets). In particular, she details more competition on privacy in the early days of social media when there was more competition to become the dominant platform. Notwithstanding this, like for any abuse of dominance case, proving that a dominant firm has abused its dominance in an anticompetitive way will remain a challenge, as noted above.

### *4.2.5. Potential efficiencies*

143. In some cases, such as in assessing mergers, it is appropriate to consider whether there are offsetting efficiencies from the conduct in question. This includes instances where privacy may be adversely affected. As noted by Manne and Sperry (2015, p. 4[111]):

> *A decrease in privacy protection is not simply a transfer from consumers to producers creating the famous deadweight loss of antitrust textbooks. Rather, the collection and use of larger amounts of information by a company like Google has the ability to improve the quality of Google's products, whether by improving the relevance of its search results or the successful targeting of its ads.*

144. Manne and Sperry (2015[111]) hence argue that any assessment of privacy as an element of quality should consider the efficiency benefits that accrue from greater data collection (in terms of better goods/services and more targeted ads) as well lower (often zero) priced goods and services. Similarly, Cooper (2013, p. 1135[125]) makes the argument that "*taking additional consumer data is not the same as skimping on quality, because collecting, storing, and analysing data is an additional cost*".

145. Further, in the case of mergers involving consumer data sets, it will also be important to consider whether the combination of data will likely bring efficiencies in the form of increased productivity in production or distribution, or the supply of tailor-made products or services (Haucap, 2019[126]). For example, one of the criticisms of the Bundeskartellamt's case against Facebook was that it did not consider the benefits that Facebook's collection of consumer data brought in terms of targeted advertising (Höppner, 2019[100]).

146. Competition agencies should ideally consider any potential efficiencies, where their legislative tests facilitate this, and to the extent that they have occurred due to the relevant conduct in question.

## 4.3. Potential remedies

147. The type of remedy that competition authorities should pursue under competition law will depend on the theory of harm.

148. In relation to mergers, both behavioural or structural remedies may be appropriate. For example, behavioural remedies could potentially restrict the merged entity's ability to combine consumer data across the merged entity. Behavioural remedies could alternatively require that access to the data set be granted to competitors under fair, reasonable and non-discriminatory (FRAND) terms. In comparison, a structural remedy may require the merged entity to divest a data set, where access to the data set raises competition concerns that cannot otherwise be addressed.[3] Alternatively, if the concern is that the merged entity will not have sufficient competitive pressure to offer competitive levels of privacy, a competition authority could block the merger to the extent that allowing it would reduce consumer welfare.

149. In practice, there are a number of examples where competition authorities have mandated data sharing as a condition of allowing a merger. For example, in allowing a merger between Ticketmaster and Live Nation, both operators in the market for primary ticketing of major concert venues, the DoJ required that the merged party provide ticketing clients with their ticketing data in a reasonably usable form upon request (DoJ, 2010[127]). That is, it required data portability (Jones Harbour and Koslov, 2010[106]). Similar remedies have been required in respect of mergers involving businesses with real estate records databases (Ohlhausen, 2019[88]).

150. In exclusionary abuse of dominance cases, similar remedies may be appropriate where the competition concern involves access to a consumer data set. The energy cases mentioned in Section 4.1.2 are relevant examples where dominant upstream players were required to provide information to potential downstream competitors to facilitate retail competition in energy markets.

151. One advantage of using competition law, rather than explicit data portability requirements to facilitate the movement of data between businesses is that competition law

[3] More generally, Line of Business Restrictions (LOBRs) will be discussed in more detail as part of the Competition Committee's Working Party 2 discussions in June 2020.

can apply to all types of data, whereas data portability tends to be limited to personal data (Graef, Verschakelen and Valcke, 2013[128]; Engels, 2016[61]). Further, as competition law is more targeted, it has the advantage that it will only impose compliance costs in cases where there is a competition concern. It also has the advantage of being more flexible than legislation, so it can adjust to the requirements of the specific market. For example, to require ongoing access to consumer data in some cases, or one-off access in others. However, competition law remedies have some drawbacks in that they are more reactive, are more likely to be litigated, and are difficult to generalise. To this end, targeted but systematic data portability requirements may be more beneficial in some markets (see Section 5.1.1). Another possible solution under competition law is to consider whether the essential facilities doctrine applies, as discussed below.

152. It is less clear how exploitative abuse of dominance cases concerning dominant players engaging in excessive consumer data collection, use and/or sharing, can be addressed through competition law remedies. In particular, like any abuse of dominance case, it will be difficult to determine what level of data protection would exist if there was more competition in the relevant market. Further, relying on consent-based models of data protection are unlikely to be particularly effective in markets with a lack of competition.

153. Last, to the extent that the theory of harm relates to a cartel or collusion, it would appear that the main remedy would be to cease the relevant conduct.

154. More generally, competition authorities should work with privacy and data protection authorities, as well as consumer authorities, to understand which type of enforcement cases to pursue, and how to develop appropriate remedies that address the identified issues (see Section 5.4).

## 4.4. The essential facilities doctrine

155. As noted by Crémer et. al. (2019, p. 73[14]), "*[t]he competitiveness of firms will increasingly depend on timely access to relevant data and the ability to use that data to develop new, innovative applications and products*". Given this, a number of commentators have considered whether data could be an "essential facility" to which the essential facilities doctrine (EFD) could potentially apply.

156. Many OECD jurisdictions have competition law provisions that allow a business to seek access to another business' assets if access is necessary to provide another good or service. The EFD, which originated in the United States in 1912, has usually been applied in respect of physical infrastructure that cannot reasonably be duplicated for technical, legal or economic reasons. Examples include ports, airports, railway networks, and water and gas pipelines. Access under the EFD is generally only granted where the access seeker cannot obtain the goods or services elsewhere and cannot build or invent them themselves, and where the owner does not have a legitimate business justification for refusing access.

157. In relation to data and the EFD in Europe, Diker Vanberg and Ünver (2017, p. 9[129]) argue that, theoretically:

> *... if a dominant company holds specific data that are indispensable for other undertakings to enter a new market, and the dominant company's refusal to transfer that data eliminates all potential competition, then, in the absence of objective justifications, Article 102 TFEU could be relied on.*

158. However, in practice, this has not been tested, and Diker Vanberg and Ünver (2017, p. 11[129]) concede that "*it would be relatively difficult for an undertaking to demonstrate why they cannot develop their own database of personal information without access to the dominant competitor's data*". In the case of online platforms, for example, Körber (2018,

p. 12[59]) argues that "*it is not at all apparent that the 'data troves' of companies such as Google or Facebook are non-duplicative, and thus essential, resources*". Further, in the United States, the courts have tended to refuse mandated access to specific databases, especially following the *Trinko* decision, which narrowed the scope of the EFD.[4]

159. To assess whether data should possibly be subject to the EFD, Lambretch and Tucker (2017[60]) considered whether data (in a general sense) are sufficiently valuable, non-imitable and rare to provide a significant and "sustainable competitive advantage". They found that for most types of data, this is unlikely to be the case. Instead, they found that access to skilled labour, and the ability to forecast future consumer demands, are more important assets than access to data in most cases. Gilbert and Pepper (2015[52]) similarly argue that, in general, access to data is not likely to be a substantial barrier to entry given data are cheap and non-rivalrous, data ownership is dispersed, historic data have little value, and data are subject to diminishing returns. They also find that the key scarcity is "human talent" to process and analyse the data.

160. However, Haucap (2019[126]) suggests that there could be good economic reasons to lower the threshold for granting third-party access to data. In particular, the fact that data is non-rivalrous means that granting access to a third party does not restrict the data controller from also using the data. This differs from many infrastructure cases in which multiple businesses are not able to use the infrastructure at the same time (for example, to dock at a port at the same time, or land on the same runway at the same time). In addition, given that the costs involved in collecting and maintaining data sets are likely to be lower, the provision of third-party access is less likely to undermine incentives for businesses to invest in data collection and maintenance of data sets.

161. As consumer data becomes more and more important, the EFD remains a possible avenue for facilitating the sharing of consumer data where this is necessary to promote competition. Theoretically, there do not appear to be any obstacles to applying the EFD to consumer data, though there remains to be a case where this has occurred, and there may be jurisprudence hurdles to overcome in doing so. It will be interesting to see how this body of law develops in respect of consumer data.

## 5. Co-operation and advocacy

162. While competition, consumer and data protection policies ultimately share a common goal to encourage better outcomes for consumers, there can be tensions in how this is put into practice. For example, competition policy does this indirectly by promoting competition, and hence, consumer welfare. In comparison, consumer and data protection policies are more concerned with protecting and empowering consumers directly.

163. For this reason, there is a role for competition advocacy in ensuring that the aims of consumer and data protection policies are not to the detriment of competition. In addition, there needs to be co-operation to ensure that the best policy lever is used where there are multiple options available.

[4] See, Verizon Communs., Inc. v. Law Offices of Curtis V. Trinko, LLP - 540 U.S. 398, 124 S. Ct. 872 (2004) (trinko). See also, Diker Vanberg and Ünver (2017[129]) for a discussion of LiveUniverse, Inc. v. MySpace, Inc., 2008 WL 5341843 (9th Cir. Dec. 22, 2008), Facebook v. Power Ventures Inc. No. 17-16161 (9th Cir. 2019), and Peoplebrowsr, Inc., et al. v. Twitter, Inc., No. C-12-6120 EMC, United States District Court, N.D. California (2013).

## 5.1. Effects of consumer data rights on competition

164. As is the case with many forms of regulation, compliance costs associated with privacy and data protection legislation can raise barriers to entry. Where these costs are largely fixed, they may disproportionately disadvantage smaller businesses. Estimates of the compliance costs of the GDPR, for example, are substantial. Costs in the United Kingdom were estimated to average GBP 1.7 million per business, ranging from just under GBP 1 million for businesses with 100-249 employees, and GBP 2.3 million for businesses with over 1 000 employees (Calgigo, 2017[130]). Even in the United States, a survey by PwC suggested that 68% of US companies would spend between USD 1 million and 10 million, and 9% of companies would spend more than USD 10 million to comply with GDPR (PwC, 2017[131]). Even for SMEs in Europe, the annual IT costs of complying with GDPR are estimated to be between EUR 3 000 and EUR 7 200 (representing 17-40% of pre-GDPR annual IT budgets) (Christensen et al., 2013[132]). This is not to say that the benefits of such regulations do not outweigh the costs, but rather that the compliance costs may affect competition in markets where businesses have to comply with these regulations. The question for competition authorities is whether the objectives of the relevant data protection legislation can be achieved in a way that minimises any (negative) impacts on competition.

165. There have also been concerns that consent-based forms of privacy regulation may advantage and entrench larger incumbents, especially those that operate across multiple markets (Campbell, Goldfarb and Tucker, 2015[133]; Marthews and Tucker, 2019[134]). This was found to be particularly pronounced in markets with less price flexibility, such as in zero-price markets (Campbell, Goldfarb and Tucker, 2015[133]). Similarly, Marthews and Tucker (2019[134]) found that the need for consent and compliance at each stage of the online advertising supply chain increases pressures for vertical integration.

166. Picker (2008, pp. 11-12[135]) raises another concern that:

> *... privacy rules that limit how information can be used and shared across firms will artificially push towards greater consolidation, something that usually works against maintaining robust competition.*

167. Further, Campbell, Goldfarb and Tucker (2015[133]) have found that opt-in consent regimes could disproportionately impact small businesses and new businesses, which they conclude would likely hinder competition. This could be more likely to occur where the compliance costs are largely fixed (irrespective of the size of the firm), making them more burdensome for smaller businesses as compared to larger businesses. As noted by Gal and Aviv (2020[110]), there may be economies of scale and scope in obtaining consumer consent. Ohlhausen (2019[88]) also found that, to the extent that privacy and data protection laws make it more difficult for businesses to acquire and use consumer data that they have not collected themselves, this might entrench incumbents that already have consent to collect and use large amounts of consumer data.

168. Early research on the impacts of GDPR suggest it has improved privacy and individuals' ability to control their data, but that it has potentially reduced competition in consumer data intensive markets. For example, on the most prominent news websites in seven European countries, the number of third-party cookies per page dropped 22% between April and July 2018 (Libert, Graves and Nielsen, 2018[136]). However, while most websites and apps still include third-party content and cookies, market shares of the larger platforms have increased under GDPR (Greif, 2018[137]). For example, ten companies tracked at least 50% of the prominent news websites in April; this had fallen to five by July (Libert, Graves and Nielsen, 2018[136]). Another study found that GDPR has led to greater concentration in online advertising in Europe (Moazed, 2019[29]).

169. Gal and Aviv (2020[110]) have found that, in addition to potentially favouring larger businesses (as discussed above), the GDPR might also reduce incentives for data sharing and might limit the use of data. In particular, the need to ensure that any party that a business shares consumer data with complies with the GDPR is an expensive undertaking that may reduce data sharing. Further, since consumer data can only be used for the purpose for which consent was originally provided, this might limit the uses to which data may be put. They conclude that these impacts are likely to reduce competition in markets that use consumer data by increasing market concentration, and reducing productive and dynamic efficiency.

170. Civot and Castro (2019[138]) have also raised concerns that the GDPR could inhibit the development and use of AI in Europe. In particular, the GDPR limits the ability of businesses to use data for any purposes other than those for which they first collected it, which could limit the ability to use consumer data in AI applications that businesses had not considered at the time of data collection. Further, there is an argument that Art. 22, which requires that automated decisions be explainable, holds such decisions to a higher standard than non-automated decisions.

171. On the other hand, to the extent that recent reforms do deliver greater levels of privacy and data control, this could potentially address some of the demand-side issues that might otherwise undermine effective competition on data protection and privacy. Moreover, if privacy regulation reduces competition while achieving its goals, policymakers may nevertheless consider it a success. What competition agencies need to focus on is whether those goals could be achieved in a way that creates fewer distortions to competition. They may also consider whether there are other pro-competitive policies that could be introduced to counterbalance the necessary damage to competition from regulating minimum standards. In practice, it may be too early to understand the full implications of a number of the reforms that have recently been implemented. In the coming years it will be important to review the effectiveness of these reforms in achieving privacy, consumer and competition outcomes. One area that is of particular interest to competition policy is data portability. This is discussed in more detail below.

### *5.1.1. Data Portability and interoperability*

172. Various examples of data portability rights were discussed in Section 2.3.2. The way in which data portability rights and responsibilities are implemented has implications for competition outcomes. For example, a number of commentators have raised concerns that data portability as envisioned under GDPR imposes high compliance costs, which when applied to non-dominant businesses, could impede competition and ultimately harm consumers (Swire and Lagos, 2013[139]; Lyons, 2018[140]). Diker Vanberg and Ünver (2017[129]) suggest that an exemption for small and medium enterprises, and undertakings with a small market share or turnover, could address this. Engles (2016[61]) goes further by suggesting that data portability should be restricted to cases where a market player has achieved a dominant position due to anticompetitive conduct.

173. Another criticism of the data portability provisions under GDPR is that, if it only provides for historic data to be transferred at one point in time, this may not facilitate multi-homing or the provision of complementary services that rely on continuous, potentially real-time, transfers of consumer data (Crémer, de Montjoye and Schweitzer, 2019[14]).

174. Further, whether it is a consumer or a (data-seeking) business (with consumer consent) that can initiate data portability will likely affect competitive outcomes (Diker Vanberg and Ünver, 2017[129]). In some use cases, demand-side barriers may limit the effectiveness of consumer-driven data portability. In particular, unless consumers

understand how to request and use data portability rights, and the benefits of using these rights, consumers may not use data portability. In this respect, the value of data portability is likely to be higher for potential competitors than for each individual consumer (Nicholas and Weinberg, 2019[141]). In particular, for businesses that require scale in terms of users – for example, in markets with network effects – consumer-driven data portability of the type envisioned under GDPR may not drive wide-scale switching (Gal and Aviv, 2020[110]). For this reason, Diker Vanberg and Ünver (2017[129]) argue instead that competition law, and in particular, the EFD (see Section 4.4) would be a more effective way of stimulating competition in markets that rely on access to data. In other cases, however, consumer-driven data portability may be more useful, for example, where there is a significant benefit from the consumer having direct access to the data and being able to move that data to another provider. For example, mobile phone number and banking portability have produced significant benefits (see Box 10).

### Box 10. Estimated benefits from portability

**Mobile number portability** has been shown to reduce market prices for mobile phone plans. One study found average price reductions of around 1% for low volume plans, 4.8% for medium-volume plans, and around 6.8% for high volume plans. Another study found decreases of between 6.6% and 12%, depending on the estimation methodology.

**Financial market portability**: The UK Payments Council launched the Current Account Switch Service (CASS) in September 2013. This voluntary scheme, covering some 40 bank and building society brands accounting for over 99% of the market, aims to make switching current accounts simpler and quicker for customers. A 2015 review of CASS found it had increased switching rates, though perhaps less than anticipated due to low consumer awareness.

**Open banking**: Research by the Centre for Economics and Business Research (Cebr) suggests that data portability enabled by open banking could result in a 7% reduction in the credit spread (risk premium add-on to the risk-free rate) on mortgages, totalling over GBP 1 billion. Based on this, Ctrl-Shift, on behalf of the UK Department for Digital, Culture, Media and Sport, estimated the economic impact of data mobility to be around GBP 28 billion across the UK economy.

Sources: Park (2011[142]); Lyons (2006[143]); FCA (2015[144]); Trustpilot (2018[145]); Ctrl-Shift (2018[146])

175. A number of businesses have offered forms of data portability for some time. For example, Facebook has allowed users to access their information via its "Download Your Information" tool since 2010 (Egin, 2019[147]). Similarly, since 2011, Google users have been able to download their personal data held by Google via its "Takeout" tool, now called "Download Your Data" (Google, 2018[148]).

176. However, there are still a number of questions about how businesses will achieve data portability as envisioned under the various regulatory regimes across the globe (Egin, 2019[147]). In particular, providing for consumer data to be transferred from one business to another (as opposed to being transferred to the consumer) raises particular issues. One key consideration is what personal data should be subject to data portability. In this respect, there seems to be some agreement that data portability should cover volunteered data and observed data (Article 29 Data Protection Working Party, 2016[149]). Further, it appears to be generally accepted that data portability should not extend to inferred data (Article 29 Data Protection Working Party, 2016[149]). However, it is unclear whether data portability

should apply to acquired data. Further, there is a trade-off between ensuring that the data provided can address lock-in, switching costs and barriers to entry, and ensuring that the data portability requirements do not undermine incentives to invest in data collection and processing. In this respect, exempting inferred data, especially from business-to-business data transfers, would appear appropriate in terms of protecting incentives for investment. However, providing this information to the individual it concerns would likely enhance informational self-determination.

177. Further, the format and content of the data will determine its usefulness in achieving informational self-determination or facilitating competition. A consumer may be overwhelmed if she receives all the data collected by a business about them, especially if this data is unstructured. However, access to an extensive range of consumer data may be extremely important for a potential competitor if the barriers to entry associated with data collection are high. As an example, Nicholas and Weinberg (2019[141]) brought together a number of individuals from the New York City tech community to see what new products they could develop with anonymised Facebook data downloaded via Facebook's Download Your Information tool. The participants found that this data was not sufficient to develop a competing social network. As noted by Nicolas and Weinberg (2019, p. 2[141]): "*trying to use exported user data to reproduce Facebook would be like trying to use furniture to reproduce the office building it came from*". Further, the participants struggled to come up with new competitive products using this information.

178. Another key consideration is how to balance the privacy of other consumers against portability requests (Egin, 2019[147]). For example, if a consumer requests portability of her data on a social media site, how can the business protect the privacy of her contacts, while still providing meaningful data for the consumer? This issue will be particularly relevant in markets where the value of the data is somewhat determined by interactions between consumers – for example, for social media networks and communications services and apps (Nicholas and Weinberg, 2019[141]). However, it will be less relevant in markets where the data only concerns an individual – for example, a consumer's music listening, fitness and video-watching preferences and habits will likely not involve other consumers. More generally, responsibilities for privacy and security during the transfer of data between businesses is an important consideration (Egin, 2019[147]).

179. Other forms of interoperability, such as protocol operability, data interoperability, and full protocol interoperability, may be more effective in facilitating competition where a continuous, potentially real-time flow of consumer data is required (Crémer, de Montjoye and Schweitzer, 2019[14]). These measures go beyond data portability and indeed may stimulate competition in adjacent markets as well as between competitors. Protocol operability refers to the development of protocols that allow systems to work together – examples include operating systems and charging protocols (between phones and charges). In comparison, data interoperability provides for real time access to data, usually in a standardised form. Of course, there are different compliance costs associated with each of these forms of interoperability. Currently, businesses usually facilitate data interoperability through proprietary APIs. Among other things, this can allow third-party developers to access the business' data to develop complementary goods or services. For example, the functionality of transport apps, such as CityMapper, Transit and Moovit, have been supported by APIs developed by transport operators, such as Transport for London (TfL), and in many cases, APIs to incorporate Google Maps (altexsoft, 2018[150]). Moreover, these transport apps have benefited from public transport organisations adopting a standard format for reporting schedules and geographic information, which encourages interoperability (Gal and Rubinfeld, 2019[26]; GTFS, n.d.[151]). Of course, these examples do not necessarily involve personal data, which raise unique challenges for privacy.

180. While APIs offer potential to increase data portability, concerns have been raised about the ability of the owner of the API to monitor and potentially block API access to potential competitors (Nicholas and Weinberg, 2019[141]). For example, there are claims that Twitter has rejected apps or revoked access to their API for apps that compete directly with it. Further, in 2012, it made changes that require API users to request special permission if their user base exceeds 100 000 (OECD, 2015[3]). Users of Facebook's Graph API have also raised concerns about Facebook monitoring and even copying their use of the API, cutting off access to the API, and changing the structure of the data (thus increasing the overheads associated with using the API) (Nicholas and Weinberg, 2019[141]). Such conduct potentially limits the competitive benefits from data interoperability through APIs.

181. New ways of facilitating data interoperability continue to be developed. For example, Apple, Facebook, Google, Windows and Twitter are currently working to create an open-source, service-to-service data portability platform through the "Data Transfer Project" (Data Transfer Project, 2018[152]). Gal and Rubinfeld (2019[26]) have also argued that the development of data standardisation could help fuel greater interoperability, lower switching costs and limit duplication, as has occurred in the public transport sector (see above). However, they also note the costs involved and the potential risk of lock-in to an inefficient standard.

182. Other ways to allow individuals to access data without impinging on privacy are also being developed. In this respect, open data rooms might offer potential in terms of a means to share consumer data while safeguarding privacy (Robertson, 2020[16]). For example, the Banque de France provides researchers with access to its Open Data Room, essentially a workstation where researchers can access a large set of anonymised granular data and aggregate series collected or produced by the Banque de France (Banque de France, 2019[153]). Data "sandboxes" have also been proposed as a way of sharing sensitive data (OECD, 2019[12]; Ctrl-Shift, 2019[154]). In addition, new frameworks for data governance might have implications for the ownership and sharing of consumer data, as discussed below.

### *5.1.2. Other approaches to data ownership and control*

183. A number of new solutions to enhancing data governance have been proposed to address problems of data ownership and control by users. Essentially, these new approaches offer a possible way to: i) internalise the externality created by an individual's demand, and capture the network effect they bring to a platform, and hence obtain greater value for individual users that generate data, and ii) facilitate collective action/switching that can actually create credible competitive threats to incumbents. For example, data trusts have been proposed as a way to facilitate the exchange of data in a "*fair, safe and equitable*" way (Hall and Pesenti, 2017[155]). As an example, the startup Streamr, which provides infrastructure for users to collectively monetise their data, has an app, Swash, which aims to facilitate a "data union" (Chakrovorti, 2020[27]). Another example is the Tide Foundation, which encrypts consumers' personal information, such that only the individual can grant access to the data, and potentially receive payment in return (Tide, 2019[156]).

184. Alternatively, Posner and Weyl (2019[157]) have proposed that data be treated as "labour" and have advocated for "data labour unions" to collectively bargain on behalf of consumers to agree arrangements and payments for access to data. Yet another venture, Ocean Protocol, intends to facilitate digital agency through a self-managed distributed ledger framework of blockchain (Chakrovorti, 2020[27]). New solutions have also been proposed for enhancing consumer identity management and verification. One such example is self-sovereign identity (see Box 11).

### Box 11. Self-sovereign Identity

Self-sovereign identity (SSI) has been proposed as a way for individuals to manage their identity. It could involve an app on a smartphone or computer – some sort of "identity wallet" – where identity data would be stored on the hard drive of the device, potentially backed up on another device or on a personal backup solution, but crucially not stored centrally (e.g. in the cloud).

The identity wallet would start off empty with only a self-generated identification number derived from a public key, and a corresponding private key (like a password, used to create digital signatures). Since the individual creates the identification number, it is self-sovereign. The identification number, along with the individual's identity claims, could then be used to get attestations from the relevant authorities.

Such attestations could serve various purposes (e.g. to signal the individual is of age, or can drive a car) and would limit the amount of information being shared with the third party. To share the relevant data or attestation, the person would approve a third party to collect specific data, perhaps via a notification on their device.

Source: Lewis (2017[158])

185. Similarly, the Unique Identification Authority of India (UIDAI) is a statutory authority that has been established to provide Unique Identification numbers (UID), named "Aadhaar", to all residents of India (UIDAI, n.d.[159]). Tim Berners-Lee, founder of the world wide web, has also been working on a solution to improve consumer control of data by decentralising the collection of consumer data and allowing consumers to control who has access to their data as part of the "Solid" project (Berners-Lee, 2018[160]). In addition, in some jurisdictions, such as Japan, "information banks" are being developed to give consumers control over how their data is used while rewarding them for sharing it (Hemmi, 2020[161]). Further, the CMA in its interim report for its market study on online platforms and digital advertising looked at various ways in which to support the development of Personal Information Management services (PIMS), Personal Data Stores (PDS), and privacy-enhancing technologies (PET) (CMA, 2019[162]). It will be important to watch how these developments progress. In particular, to ensure that there are no competitive or legislative barriers to their development and adoption.

## 5.2. The role of consumer policy

186. As discussed in Section 3.3.1, one of the possible market failures associated with the provision of privacy and consumer data is asymmetric information. To the extent that there is a problem of asymmetric information, there may be a role for consumer policy enforcement rather than competition enforcement. Specifically, if businesses abuse asymmetric information to mislead or deceive consumers, this could potentially be addressed under consumer policy. For example, the OECD's *Recommendation on Consumer Protection in E-Commerce* states that businesses should not mislead or deceive consumers, including in relation to the collection and use of consumers' personal data (OECD, 2016[163]). It also states that businesses should not engage in unfair practices nor use unfair contract terms (OECD, 2016[163]). Most OECD member countries have enacted consumer laws to give effect to these recommendations.

187. Ohlhausen and Okuliar (2015[164]) argue that consumer protection laws are a much better way to protect consumers in respect of privacy, rather than trying to pursue privacy

objectives through competition law enforcement. In practice, a number of consumer authorities have taken enforcement cases related to businesses' privacy and personal data practices, as outlined in the OECD's "Good Practice Guide on Consumer Data" (2019[13]). In respect of deceptive conduct regarding a business' privacy and data security practices, there are examples from the United States, where the FTC has taken cases against Uber, a ride-sharing app; Facebook, a social networking app (see Box 12); a marketing company, and; a technology provider (OECD, 2019[13]). Deception can also occur due to misrepresentation by omission. Cases of this type in respect of data practices have been taken in the United States, Norway, Australia, Canada, Hungary, the United Kingdom, Italy (in respect of Facebook – see Box 12) and by the EC (OECD, 2019[13]). Some jurisdictions also have the ability to take enforcement action in respect of "unfair" consumer data practices. Such cases have been taken in the United States and by the EC (OECD, 2019[13]).

### Box 12. Enforcement against Facebook's privacy practices under consumer law

In the **United States**, the FTC has taken a number of cases against Facebook in relation to its privacy and personal data practices. In 2012, it reached a settlement with Facebook in respect of eight counts of conduct that it viewed were unfair methods of competition. In 2019, it imposed a USD 5 billion penalty on Facebook for violating the 2012 order by deceiving users about their ability to control the privacy of their personal information. In addition, it imposed a 20 year settlement order to overhaul "*the way the company makes privacy decisions by boosting the transparency of decision making and holding Facebook accountable via overlapping channels of compliance*".

In **Italy** in 2018, the Italian competition authority (AGCM) found Facebook responsible of two unfair commercial practices in breach of the Italian Consumer Code for its privacy and data collection practices. First, the AGCM considered that Facebook mislead users regarding the collection and use of consumer data during the registration process since it considered that the information provided lacked immediacy, clarity and completeness. Specifically, the AGCM challenged Facebook's claim that its social network is "*free and always will be*" as false given that consumers provide their data in using the service. Second, it found that Facebook's data sharing practices were "aggressive" in that it shared consumer data with third-party websites and apps without prior and express consumer consent. It imposed a EUR 5 million fine for each infringement – EUR 10 million in total.

Facebook appealed the decision to the regional Administrative Court of Lazio, who in 2020, agreed with the AGCM in respect of the first charge but overturned the second, and consequently reduced the total fine to EUR 5 million. In respect of the first charge, the court confirmed the AGCM's ruling that personal data can be considered as a negotiable asset susceptible to economic exploitation. Hence, personal data can be considered as "counter-performance" in a contract.

Sources: FTC (2012[165]); FTC (2019[166]); FTC (2019[167]); AGCM (2018[168]); Monga (2020[169]); Asaro and Thiem (2020[170]), Il Tribunale Amministrivo Regionale per il Lazio (2020[171])

## 5.3. Is there a role for economic regulation?

188. In addition to using competition, privacy, and consumer protection laws to address market failures associated with consumer data and privacy, some commentators have suggested there may be a role for specific economic regulation in certain markets that rely

on consumer data. Crémer et. al. (2019, p. 74[14]) conclude, in respect of data generally, that:

> *When it comes to ensuring access to data for the purpose of promoting AI in general in order to foster innovation – i.e. a form of data access that is unrelated to the business activity of the data controller – we believe that a legal regime outside of competition law will be needed.*

189. Further, Colangelo and Maggiolino (2018[98]) argue that if the concern associated with a lack of data protection in online platforms is one of market structure (e.g. because many online platforms are multi-sided markets with network effects that may lend themselves to market concentration), economic regulation may be a more appropriate policy response than antitrust law. In addition, to the extent that there are substantial externalities associated with the collection and use of consumer data, this might suggest that economic regulation is a more appropriate policy tool, so long as the benefits outweigh the costs. For example, given that externalities associated with the use of data can be positive or negative depending on how data is used, Gal and Rubinfeld (2019[26]) suggest that perhaps a better form of regulation may be to regulate the ways in which data is used (i.e. to limit or restrict data uses that are likely to result in negative externalities).

190. In Europe, the EC has adopted sector-specific legislation in respect of data in the automotive industry; payment service providers' data; smart metering data; electricity network data, and; intelligent transport systems data (European Commission, 2020[1]).

191. A number of jurisdictions have also looked at establishing specific work units to consider how best to regulate digital platforms, including their use of consumer data. For example, the 2019 "Furman report" on "Unlocking digital competition" in the United Kingdom, recommended the establishment of a "Digital Markets Unit" (DMU) (Furman et al., 2019[70]). The DMU would exist as part of the CMA or Ofcom (or an independent body linking the two). It would have a remit to use tools and frameworks to support greater competition and consumer choice in digital markets, backed by new powers in legislation. One of its first tasks would be to establish a code of conduct, which would apply to businesses that are deemed to have "strategic market status". In addition, it would be tasked with enabling greater personal data mobility and systems with open standards where these tools will increase competition and consumer choice. Similarly, in the United States, the "Stigler review" (2019[172]) recommended that a single regulator be formed to oversee open standards, data portability and access, monitor the use of "dark patterns" and the risks of addiction, and to assist the FTC and DoJ in undertaking merger reviews in digital markets. In addition, the Danish Competition and Consumer Authority and the ACCC have both established digital platform units in the last two years.

## 5.4. The need for co-operation

192. The need for co-operation and coordination across agencies when issues span multiple policy domains was flagged in the OECD's report on "Quality Considerations in the Zero-Price Economy". In particular, it noted that (OECD, 2018, p. 31[6]):

> *… a rigid separation between the sphere of action of competition, consumer protection and data protection authorities would most likely not lead to optimal outcomes, in terms of both consumer welfare and consumer protection. For this reason, the three policy areas may need to be applied in parallel …*

193. While this observation was made in the context of zero-price markets, it is equally valid when talking about ensuring that levels of data protection and the collection and use of consumer data are to the benefit of consumers, and to competition in markets.

Co-operation across competition, consumer and privacy domains was also a central theme of the EDPS's 2014 "Preliminary opinion on privacy and competitiveness in the age of big data" and its 2016 "Opinion on coherent enforcement of fundamental rights in the age of big data" (EDPS, 2014[30]; EDPS, 2016[173]). This latter opinion recommended a closer dialogue between regulators and experts across policy boundaries, with the goal of strengthening competition and consumer protection enforcement and stimulating the market for privacy-enhancing services. Kerber (2016[174]) went further, arguing for the development of a "common strategy" across these three policy areas. Such an approach may be easier to implement where a competition authority has a broader remit including consumer protection, data protection and/or sectoral regulation, for example.

194. In respect of coordinating competition and consumer policy issues and enforcement, this is more straightforward in the 30 plus jurisdictions that have these responsibilities tasked to one common agency (Kovacic and Hyman, 2013[175]). In addition, legislative provisions can provide the legal basis for co-operation between competition, data protection and consumer authorities. In Germany, for example, amendments to the *Act Against Restraints on Competition*, which came into force in June 2017, provide for this (Stauber, 2019[176]). In particular, under s. 50c(1), Federal and state competition and data protection authorities can exchange information, including personal data and operating and business secrets, to the extent that this is necessary for the performance of their respective functions, and use such information in their proceedings. Co-operation between the relevant authorities in the Bundeskartellamt's case against Facebook was of key import, for example. In addition, in Australia, co-operation has been built into the new CDR with the ACCC, OAIC and the DSB being jointly responsible for its implementation (see Box 4).

195. Less formal means of co-operating are also available. For example, the EDPS's 2016 opinion recommended that a "Digital Clearinghouse" be created to facilitate information sharing between regulators dealing with online markets (see Box 13).

### Box 13. Europe's Digital Clearinghouse

In 2016, the EDPS published an "Opinion on coherent enforcement of fundamental rights in the age of big data", which recommended establishing a "Digital Clearinghouse" to coordinate enforcement across Europe's digital sector. It was envisioned that the Digital Clearinghouse would be a voluntary network of regulators involved in the enforcement of legal regimes in digital markets, with a focus on data protection, consumer and competition laws. In a 2017 Resolution, the European Parliament endorsed the establishment and development of the Digital Clearinghouse as envisioned by the EDPS, noting that it could "*help deepen the synergies and the safeguarding of the rights and interests of individuals*".

The objectives of the Digital Clearinghouse are to (i) exchange best practices and novel ideas about how to protect individuals in digital markets across legal regimes, and (ii) bring together different stakeholders involved in this challenge. The EDPS hosted four meetings of the Digital Clearinghouse between 2017 and 2018. From 2019, it has been jointly hosted by the Research Centre in Information, Law and Society (CRIDS) at the University of Namur, the Tilburg Institute for Law, Technology, and Society (TILT) at Tilburg University, and the European Policy Centre (EPC) in Brussels. All regulators in the digital space from across the globe are invited and able to participate.

Sources: Digital Clearinghouse (n.d.[177]); EDPS (2016[173]); European Parliament (2017[178]); EDPS (n.d.[179]).

196. Market studies also offer potential in terms of understanding the broader policy issues in particular markets (OECD, 2018[6]). These can be particularly useful in understanding demand-side concerns that would ordinarily tend to fall outside the scope of competition authorities' enforcement mandates. As discussed in Section 4.2.3, demand-side issues are of particular relevance to privacy, both in relation to problems of asymmetric information and behavioural biases. Working across competition, consumer and privacy policy areas might hence be a more effective means of delivering beneficial policy change in this area rather than looking at it through one policy lens.

## 6. Conclusions

197. This paper explores some of the difficulties associated with incorporating consumer data considerations into competition policy and enforcement. While consumer data has been used by businesses for some time, and privacy has arguably always been of some importance to consumers, these issues are only going to become more relevant to competition enforcement and policy.

198. There is growing support for the notion that competition authorities should consider privacy and data protection as a potential aspect of competition on quality in assessing competition enforcement cases in markets involving consumer data. However, this is difficult in practice. While competitive pressures should lead to competition on privacy at least theoretically, there may be demand-side obstacles to effective competition in practice, even in markets where consumers say they care about privacy. In particular, consumer understanding about privacy and data collection and use practices is often low. This asymmetry in information could lead to an "adverse selection" problem in the provision of privacy in relevant markets. In this case, consumer and data protection regulation and enforcement may be a better response compared to competition enforcement if the goal is to ensure a minimum level of data protection. Nonetheless, there may be cases in which businesses do compete on privacy and competition authorities should factor this into competition assessments. This is likely to be especially the case in mergers enforcement, especially if one of the parties is a maverick firm when it comes to their privacy practices. In such cases, consumer and business surveys about the importance of privacy in the market, as well as market (i.e. consumer and business) responses to changes in the level of privacy offered in the market may provide useful supporting evidence.

199. There are also circumstances where consumer data may confer a competitive advantage on certain market players. In particular, where a business has unique access to certain types of consumer data. To the extent that a merger would consolidate such an advantage, this is a relevant consideration in merger assessments. Further, if a dominant business is restricting access to its data, this may also be a relevant consideration under competition law. Similarly, if a dominant business uses tying or bundling to maintain or leverage its dominance in respect to access and use of consumer data, this is also relevant to competition law. A key issue in such cases is to assess the barriers to entry in the relevant markets, which will necessarily have to consider the specific characteristics of the relevant market. To the extent that access to a specific consumer data set is essential to fostering competition, there may also be a role for the EFD, which to date is largely untested in relation to consumer data. More generally, to the extent that access to consumer data addresses concerns raised in relation to a merger, or an abuse of dominance, this remains an option under competition law. Alternatively, there may be remedies available under other policy domains such as privacy and data protection policies.

200. In particular, rights to data portability might foster competition if these are designed and implemented with potential impacts on barriers to entry and demand-side impediments

to the use of such rights, in mind. In particular, the implementation and compliance costs of data portability can be high and the use case for consumers may be limited, so from a competition perspective, a targeted approach to data portability requires further consideration. There is also a role for competition advocacy to ensure that privacy and data protection regulations more broadly do not have perverse outcomes for competition, for example by raising barriers to entry unnecessarily. It is recommended that such regulations be reviewed after implementation to assess their competitive and broader impacts in various markets. Some issues, such as asymmetric and misleading information, should potentially be addressed under consumer rather than competition policy. The question remains about whether there are certain markets in which market structures are such that economic regulation may be more appropriate than competition regulation. In assessing these various issues and trade-offs, it is important that competition, consumer and data protection authorities share information and ideas both in developing and advocating for policy change, and in taking enforcement action.

201. In summary, competition authorities have a role to play in promoting privacy and ensuring that access to and use of consumer data does not result in poor outcomes for consumers where these are important aspects of competition in the relevant markets. However, this is still a relatively new area of competition policy where the relevant theories of harm are still largely untested. Further, as with other competition assessments involving quality, the economic models are less well developed and accepted as those based on price effects. In the coming years, competition agencies will need to continue to invest in understanding the competitive dynamics in markets involving consumer data, and to continue to collaborate and co-operate with enforcement and policy agencies with responsibilities for data protection and consumer policy in particular.

# *References*


ACCC (2019), *Customer Loyalty Schemes: Final Report*, https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF. [40]

ACCC (2019), *Digital Platforms Inquiry: Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf. [58]

ACCC (n.d.), *Consumer data right (CDR)*, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0. [35]

Acquisti, A., C. Taylor and L. Wagman (2016), "The Economics of Privacy", *Journal of Economic Literature*, Vol. 54/2, pp. 442-492, http://dx.doi.org/10.1257/jel.54.2.442. [15]

Adams, M. (2014), *The Origins of Personal Data and its Implications for Governance*, The Information Accountability Foundation, http://dx.doi.org/10.2139/ssrn.2510927. [180]

AGCM (2018), *Facebook – condivisione dati con terzi*. [168]

Akerlof, G. (1970), "The Market for ''Lemons'': Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84/3, pp. 488-500, http://links.jstor.org/sici?sici=0033-5533%28197008%2984%3A3%3C488%3ATMF%22QU%3E2.0.CO%3B2-6 (accessed on 6 July 2017). [67]

altexsoft (2018), *Public Transportation Apps' APIs and Platforms: Maps, Scheduling, Trip Planning, and Mobile Ticketing*, https://www.altexsoft.com/blog/engineering/public-transportation-apps-apis-and-platforms-maps-scheduling-trip-planning-and-mobile-ticketing/. [150]

Anderson, K. (2019), "Mass Market Consumer Fraud in the United States: A 2017 Update", *Staff Report of the Bureau of Economics*, Federal Trade Commission. [62]

Arthur, C. (2011), *What's a zettabyte? By 2015, the internet will know, says Cisco*, https://www.theguardian.com/technology/blog/2011/jun/29/zettabyte-data-internet-cisco. [2]

Article 29 Data Protection Working Party (2016), *Guidelines on the right to data portability*. [149]

Asaro, A. and T. Thiem (2020), *Facebook is not free: The regional Administrative Court of Lazio affirms the commercial value of the personal data of the social network users*, https://www.lexology.com/library/detail.aspx?g=7daa5f60-dfe0-41dd-9a15-34aa7e499a2e. [170]

Autorité de la concurrence (2014), *Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité*, https://www.autoritedelaconcurrence.fr/sites/default/files/2019-10/14mc02.pdf. [94]

Auxier, B. et al. (2019), *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. [113]

Bakhoum, M. et al. (eds.) (2018), *The Rise of Big Data and the Loss of Privacy*, Springer, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795992. [101]

Banco Central do Brasil (2019), *The revitalized Positive Credit Report has become fully operational*, https://www.bcb.gov.br/en/pressdetail/2279/nota. [103]

Banque de France (2019), *Open Data Room*, https://www.banque-france.fr/en/statistics/access-granular-data/open-data-room. [153]

Bartz, D. and D. Lawsky (2008), *Google clout seen aiding Microsoft antitrust OK*, https://www.reuters.com/article/businesspro-microsoft-yahoo-antitrust-dc/google-clout-seen-aiding-microsoft-antitrust-ok-idUSN0144485520080202. [188]

Beales, J. (2019), *Public Goods, Private Information: Providing an Interesting Internet*, p. 14, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/04/AC-April-02.pdf. [185]

Beal, V. (2008), *What are Internet Cookies and What Do They Do?*, Webopedia, https://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp (accessed on 11 January 2018). [41]

Berners-Lee, T. (2018), *One Small Step for the Web…*, https://inrupt.com/blog/one-small-step-for-the-web. [160]

Binns, R. and E. Biettib (2019), "Dissolving privacy, one merger at a time: Competition, data and third party tracking", *Computer Law & Security Review*, https://doi.org/10.1016/j.clsr.2019.105369. [50]

Binns, R. et al. (2018), *Third Party Tracking in the Mobile Ecosystem*, http://dx.doi.org/10.1145/3201064.3201089. [47]

Boerman, S., S. Kruikemeier and F. Zuiderveen Borgesius (2017), "Online Behavioral Advertising: A Literature Review and Research Agenda", *Journal of Advertising*, Vol. 46/3, pp. 363-376, http://dx.doi.org/10.1080/00913367.2017.1339368. [44]

Bundeskartellamt (2019), *Bundeskartellamt prohibits Facebook from combining user data from different sources*, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html. [96]

Bundeskartellamt (2019), *Decision of the Bundeskartellamt B6-22/16 regarding Facebook*, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5. [95]

Bundeskartellamt and Autorité de la concurrence (2016), *Competition Law and Data*, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.html. [69]

CADE (2016), *CADE approves with restrictions joint venture between banks in the sector of credit information services*, http://www.cade.gov.br/cade_english/press-releases/cade-approves-with-restrictions-joint-venture-between-banks-in-the-sector-of-credit-information-services. [104]

Calgigo (2017), *The Clock is Ticking: The Truth About GDPR Compliance*, https://calligo.cloud/resources/ebook/the-truth-about-gdpr-compliance/. [130]

Calo, R. (2014), "Digital Market Manipulation", *The George Washington Law Review*, Vol. 82/4, pp. 995-1051, http://www.gwlr.org/wp-content/uploads/2014/10/Calo_82_41.pdf (accessed on 30 January 2018). [63]

Calo, R. and A. Rosenblat (2017), "The Taking Economy: Uber, Information, and Power", *Columbia Law Review*, Vol. 117, http://dx.doi.org/10.1111/soc4.12493. [64]

Campbell, J., A. Goldfarb and C. Tucker (2015), "Privacy Regulation and Market Structure", *Journal of Economic & Management Strategy*, Vol. 24/1, pp. 47-73, http://dx.doi.org/10.1111/jems.12079. [133]

Carrascal, J. (2011), *Your browsing behavior for a Big Mac: Economics of Personal Information*, https://www.researchgate.net/publication/51968495_Your_browsing_behavior_for_a_Big_Mac_Economics_of_Personal_InformationOnline. [187]

Chakrovorti, B. (2020), *Why It's So Hard for Users to Control Their Data*, https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data. [27]

Chiou, L. and C. Tucker (2017), *Search Engines and Data Retention: Implications for Privacy and Antitrust*, https://www.nber.org/papers/w23815. [109]

Chivot, E. and D. Castro (2019), *The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy*, https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/. [138]

Choi, J., D. Jeon and B. Kim (2019), "Privacy and personal data collection with information externalities", *Journal of Public Economics*, Vol. 173, https://doi.org/10.1016/j.jpubeco.2019.02.001. [68]

Christensen, L. et al. (2013), *The Impact of the Data Protection Regulation in the E.U.*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138&rep=rep1&type=pdf. [132]

Cisco (2019), *Consumer Privacy Report: The growing imperative of getting of getting data privacy right*, https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf. [112]

CMA (2019), *Appendix L: Potential approaches to improving personal data mobility*, https://assets.publishing.service.gov.uk/media/5df9efa2ed915d093f742872/Appendix_L_Potential_approaches_to_improving_personal_data_mobility_FINAL.pdf#page=10. [162]

CMA (2016), *Energy Market Investigation*, https://assets.publishing.service.gov.uk/media/5773de34e5274a0da3000113/final-report-energy-market-investigation.pdf. [93]

CMA (2015), *The commercial use of consumer data*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf. [28]

Cohen, J. (2013), "What Privacy is For", *Havard Law Review*, Vol. 126, p. 1904, https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf. [65]

Colangelo, G. and M. Maggiolino (2018), "Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S.", *Stanford Law School and the University of Vienna School of Law TTLF Workin*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125490. [98]

Commission, F. (ed.) (2014), *FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition*, https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed. [85]

Condorelli, D. and J. Padilla (2019), *Harnessing Platform Envelopment Through Privacy Policy Tying*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504025. [71]

Cooper, J. (2013), *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, https://www.law.gmu.edu/assets/files/publications/working_papers/1339PrivacyandAntitrust.pdf. [125]

Costa-Cabral, F. and O. Lynskey (2017), "Family ties: the intersection between data protection and competition in EU Law", *Common Market Law Review*, Vol. 54/1, pp. 11-50, http://www.kluwerlawonline.com/abstract.php?area=Journals&id=COLA2017002. [105]

CPI (2019), *Germany: Facebook succeeds in blocking German ban on data collection*, https://www.competitionpolicyinternational.com/germany-cartel-office-to-take-facebook-case-to-high-court/. [97]

Crémer, J., Y. de Montjoye and H. Schweitzer (2019), *Competition Policy for the Digital Era*, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf. [14]

Ctrl-Shift (2019), *Personal Data Mobility Sandbox report*, https://www.ctrl-shift.co.uk/news/2019/06/17/release-of-data-mobility-infrastructure-sandbox-report/. [154]

Ctrl-Shift (2018), *Data Mobility: The personal data portability growth opportunity for the UK economy*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755219/Data_Mobility_report.pdf. [146]

Data Transfer Project (2018), *Data Transfer Project Overview and Fundamentals*, https://datatransferproject.dev/dtp-overview.pdf. [152]

Department for Business, Innovation & Skills (2011), *The midata vision of consumer empowerment*, https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment (accessed on 20 February 2020). [33]

Digital Clearinghouse (n.d.), *Digital Clearinghouse*, https://www.digitalclearinghouse.org/. [177]

Diker Vanberg, A. and M. Ünver (2017), "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", *European Journal of Law and Technology*, Vol. 8/1, http://ejlt.org/article/view/546/727. [129]

DoJ (2010), *Justice Department Requires Ticketmaster Entertainment Inc. to Make Significant Changes to Its Merger with Live Nation Inc.*, https://www.justice.gov/opa/pr/justice-department-requires-ticketmaster-entertainment-inc-make-significant-changes-its. [127]

EC (2018), *Apple/Shazam*, https://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf. [92]

EC (2016), *Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions*, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284. [90]

EC (2016), *Sanofi / Google / DMI JV*, https://ec.europa.eu/competition/mergers/cases/decisions/m7813_479_2.pdf. [91]

EC (2008), *TomTom/Tele Atlas*, https://ec.europa.eu/competition/mergers/cases/decisions/m4854_20080514_20682_en.pdf. [75]

EDPS (2016), *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf. [173]

EDPS (2014), *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en. [30]

EDPS (n.d.), *Big Data & Digital Clearinghouse*, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en. [179]

Egin, E. (2019), *Charting a Way Forward: Data Portability and Privacy*, Facebook, https://iapp.org/media/pdf/fb_whitepaper_sep_2019.pdf. [147]

Engels, B. (2016), "Data portability among online platforms", *Internet Policy Review*, Vol. 5/2, http://dx.doi.org/10.14763/2016.2.408. [61]

Esayas, S. (2018), *Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232701. [122]

European Commission (2020), *A European strategy for data*, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. [1]

European Commission (2017), *Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover*, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369. [83]

European Commission (2016), *Case M.8124 – Microsoft/LinkedIn*, https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf. [89]

European Commission (2014), *Case No COMP/M.7217 - Facebook/WhatsApp*, https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf. [80]

European Commission (2012), *Case No COMP/M.6314 – Telefónica UK/Vodafone UK/ Everything Everywhere/ JV*, https://ec.europa.eu/competition/mergers/cases/decisions/m6314_20120904_20682_2898627_EN.pdf. [76]

European Commission (2008), *Case No COMP/M.4731 – Google/ DoubleClick*, https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf. [72]

European Court of Justice (2006), *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62005CJ0238&from=EN. [102]

European Parliament (2017), *Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*, https://www.europarl.europa.eu/doceo/document/A-8-2017-0044_EN.pdf. [178]

Ezrachi, A. and V. Roberston (2019), "Competition, Market Power and Third-Party Tracking", *World Competition*, Vol. 42/1, pp. 5-20, https://www.kluwerlawonline.com/abstract.php?area=Journals&id=WOCO2019002. [49]

Farrell, J. (2012), "Can privacy be just another good?", *Journal on Telecommunications and High Technology Law*, Vol. 10, pp. 251-265, http://www.jthtl.org/content/articles/V10I2/JTHTLv10i2_Farrell.PDF. [121]

FCA (2015), *Making current account switching easier: The effectiveness of the Current AccountSwitch Service (CASS) and evidence on account number portability*, https://www.fca.org.uk/publication/research/making-current-account-switching-easier.pdf. [144]

Federal Trade Commission (2007), *Statement of the Federal Trade Commission concerning Google/DoubleClick*, https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. [73]

fieldfisher (ed.) (2019), *CCPA Blog Series, Part 2: Rethinking access and data portability rights*, https://privacylawblog.fieldfisher.com/2019/ccpa-blog-series-part-2-rethinking-access-and-data-portability-rights. [36]

Forrest, K. (2019), *Big Data and Online Advertising: Emerging Competition Concerns*, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/04/AC-April-02.pdf. [107]

FTC (2019), *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (accessed on 17 February 2020). [167]

FTC (2019), *Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson In re Facebook, Inc.*, https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf. [166]

FTC (2017), *Cross-Device Tracking*, https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (accessed on 26 March 2018). [43]

FTC (2014), *Early Termination Notice: 20140457: Google Inc.; Nest Labs, Inc.*, https://www.ftc.gov/enforcement/premerger-notification-program/early-termination-notices/20140457. [86]

FTC (2012), *FTC Approves Final Settlement With Facebook: Facebook Must Obtain Consumers' Consent Before Sharing Their Information Beyond Established Privacy Settings*, https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook (accessed on 17 February 2020). [165]

FTC (2012), *FTC Closes Its Investigation Into Facebook's Proposed Acquisition of Instagram Photo Sharing Program*, https://www.ftc.gov/news-events/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition. [79]

Furman, J. et al. (2019), *Unlocking digital competition: Report of the Digital Competition Expert Panel*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf. [70]

Gal, M. and O. Aviv (2020), "The Competitive Effects of the GDPR", *Journal of Competition Law and Economics*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444. [110]

Gal, M. and D. Rubinfeld (2019), *Data Standardization*, pp. 737-770, https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-GalRubinfeld-1.pdf. [26]

Gilbert, P. and R. Pepper (2015), *Privacy Considerations in European Merger Control: A Square Peg for a Round Hole*, Competition Policy International, https://www.competitionpolicyinternational.com/assets/Uploads/PepperGilbertMay-152.pdf. [52]

González Fuster, G., R. van Brakel and P. De Hert (eds.) (2019), *Data Protection and Competition Law: The Dawn of 'Uberprotection'*, Edward Elgar Publishing, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290824. [77]

Google (2018), *Introducing Data Transfer Project: an open source platform promoting universal data portability*, https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html. [148]

Graef, I., J. Verschakelen and P. Valcke (2013), "Putting the right to data portability into a competition law perspective", *Law: The Journal of the Higher School of Economics, Annual Review.*, https://www.researchgate.net/publication/281092445_Putting_the_right_to_data_portability_into_a_competition_law_perspective. [128]

Greif, B. (2018), *Study: Google Is the Biggest Beneficiary of the GDPR*, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr. [137]

GTFS (n.d.), *GTFS: Making Public Transit Data Universally Accessible*, https://gtfs.org/. [151]

Hall, D. and J. Pesenti (2017), *Growing the Artificial Intelligence Industry in the UK*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf. [155]

Haucap, J. (2019), *Data protection and antitrust: new types of abuse cases? An economist's view in light of the German Facebook decision*, Competition Policy International, pp. 24-29, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf. [126]

Hemmi, J. (2020), *Japan's 'information banks' to let users cash in on personal data*, https://asia.nikkei.com/Business/Business-trends/Japan-s-information-banks-to-let-users-cash-in-on-personal-data. [161]

Honey, K., P. Chrousos and T. Black (2016), *My Data: Empowering All Americans with Personal Data Access*, https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access (accessed on 20 February 2020). [31]

Hoofnagle, C. and J. Whittington (2014), "Free: Accounting for the Costs of the Internet's Most Popular Price", *UCLA Law Review*, Vol. 61, pp. 606-670, https://www.uclalawreview.org/pdf/61-3-2.pdf. [117]

Höppner, T. (2019), *Data Exploiting as an Abuse of Dominance: The German Facebook Decision*, Hausfeld, https://www.hausfeld.com/news-press/data-exploiting-as-an-abuse-of-dominance-the-german-facebook-decision. [100]

Hull, G. (2014), "Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data", *Ethics and Information Technology*, Vol. 17/2, pp. 89-101, http://dx.doi.org/10.2139/ssrn.2533057. [116]

IAB (2013), *Cookies on Mobile 101*, https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf (accessed on 26 March 2018). [42]

Il Tribunale Amministrativo Regionale per il Lazio (2020), *Altroconsumo, National Consumers' Union and Citizen's Defence Movement v. Facebook*, https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=tar_rm&nrg=201815288&nomeFile=202000261_01.html&subDir=Provvedimenti. [171]

ISO/IEC (2018), *Privacy enhancing data de-identification terminology and classification of techniques*, http://www.iso.org/standard/69373.html. [23]

Jones Harbour, P. (2007), *Dissenting Statement of Commissioner Pamela Jones Harbour: In the Matter of Google/DoubleClick*, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf. [74]

Jones Harbour, P. and T. Koslov (2010), "Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets", *Antitrust Law Journal*, Vol. 76/3, pp. 769-797, https://www.jstor.org/stable/40843729?seq=1. [106]

Këllezi, P. (2019), *Data Protection and Competition Law: Non-Compliance as Abuse of Dominant Position*, p. 343, https://ssrn.com/abstract=3503860. [99]

Kemp, K. (2019), "Concealed Data Practices and Competition Law: Why Privacy Matters", *University of New South Wales Law Research Series*, Vol. 53/Research Paper No. 19-53, http://dx.doi.org/10.2139/ssrn.3432769. [17]

Kerber, W. (2019), "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 9, pp. 310-331, https://www.jipitec.eu/issues/jipitec-9-3-2018/4807/JIPITEC_9_3_2018_310_Kerber. [51]

Kerber, W. (2016), "Digital markets, data, and privacy: competition law, consumer law and data protection", *Journal of Intellectual Property Law & Practice*, p. jpw150, http://dx.doi.org/10.1093/jiplp/jpw150. [174]

Kokolakis, S. (2017), "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", *Computers & Security*, Vol. 64, pp. 122-134, http://dx.doi.org/10.1016/j.cose.2015.07.002. [119]

Körber, T. (2018), "Is Knowledge (Market) Power? - On the Relationship Between Data Protection, 'Data Power' and Competition Law", *NZKart 2016*, pp. 303-348, https://ssrn.com/abstract=31122. [59]

Kovacic, W. and D. Hyman (2013), "Competition Agencies with Complex Policy Portfolios: Divide or Conquer?", *GW Law Faculty Publications & Other Works*, p. 631, https://scholarship.law.gwu.edu/faculty_publications/631/. [175]

Lambretch, A. and C. Tucker (2017), *Can Big Data Protect a Firm from Competition?*, https://www.competitionpolicyinternational.com/wp-content/uploads/2017/01/CPI-Lambrecht-Tucker.pdf. [60]

Lewis, A. (2017), *A gentle introduction to self-sovereign identity*, https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/. [158]

Libert, T., L. Graves and R. Nielsen (2018), *Changes in Third-Party Content on European News Websites after GDPR*, https://reutersinstitute.politics.ox.ac.uk/our-research/changes-third-party-content-european-news-websites-after-gdpr (accessed on 20 February 2020). [136]

Lynskey, O. (2018), *Non-price Effects of Mergers*, OECD Publishing, https://one.oecd.org/document/DAF/COMP/WD(2018)70/en/pdf. [82]

Lyons, D. (2018), *GDPR: Privacy as Europe's tariff by other means?*, https://www.aei.org/technology-and-innovation/gdpr-privacy-as-europes-tariff-by-other-means/. [140]

Lyons, S. (2006), *Measuring the Benefits of Mobile Number Portability*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.571.9222&rep=rep1&type=pdf. [143]

Maggiolino, M. and G. Ferrari (2020), *Can Digital Data be Replaced? Data*, Competition Policy International, p. 37, https://www.competitionpolicyinternational.com/wp-content/uploads/2020/02/AC-February-II.pdf. [56]

Manne, G. and R. Sperry (2015), "The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework", *CPI Antitrust Chronicle*, Vol. 2, https://www.competitionpolicyinternational.com/assets/Uploads/ManneSperryMay-152.pdf. [111]

Marr, B. (2016), *What Is The Difference Between Artificial Intelligence And Machine Learning?*, https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/. [55]

Marthews, A. and C. Tucker (2019), *Privacy policy and competition*, https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf. [134]

Moazed, A. (2019), *How GDPR is Helping Big Tech and Hurting the Competition*, https://www.applicoinc.com/blog/how-gdpr-is-helping-big-tech-and-hurting-the-competition/. [29]

Monga, G. (2020), *Italian Court says that personal data submitted to Facebook are economic assets*, https://www.mmlex.it/en/magazine/italian-administrative-court-lazio-confirms-personal-data-are-economic-asset. [169]

Nicholas, G. and M. Weinberg (2019), *Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?*, https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition. [141]

Norberg, P., D. Horne and D. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *The Journal of Consumer Affairs*, Vol. 41/1, pp. 100-126, http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x. [118]

Ocello, E., C. Sjödin and A. Subočs (2015), *What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case*, European Commission, https://ec.europa.eu/competition/publications/cmb/2015/cmb2015_001_en.pdf. [81]

OECD (2020), *Conglomerate effects of mergers*, http://www.oecd.org/daf/competition/conglomerate-effects-of-mergers.htm. [10]

OECD (2020), *Digital disruption in financial markets*, https://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm. [8]

OECD (2020), *Start-ups, killer acquisitions and merger control*, http://www.oecd.org/daf/competition/start-ups-killer-acquisitions-and-merger-control.htm. [9]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, http://dx.doi.org/10.1787/276aaca8. [12]

OECD (2019), *Good practice guide on consumer data*, OECD Publishing, http://dx.doi.org/10.1787/20716826. [13]

OECD (2019), *Online Advertising: Trends, benefits and risks for consumers*, http://dx.doi.org/10.1787/20716826. [45]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*. [53]

OECD (2018), *IoT measurement and applications*, OECD Publishing, http://dx.doi.org/10.1787/20716826. [21]

OECD (2018), *Non-price effects of mergers*, https://www.oecd.org/daf/competition/non-price-effects-of-mergers.htm (accessed on 14 February 2020). [5]

OECD (2018), *Personalised Pricing in the Digital Era*, https://www.oecd.org/daf/competition/personalised-pricing-in-the-digital-era.htm (accessed on 14 February 2020). [7]

OECD (2018), *Quality considerations in the zero-price economy*, https://www.oecd.org/daf/competition/quality-considerations-in-the-zero-price-economy.htm (accessed on 14 February 2020). [6]

OECD (2018), *Rethinking Antitrust Tools for Multi-Sided Platforms*, https://www.oecd.org/daf/competition/Rethinking-antitrust-tools-for-multi-sided-platforms-2018.pdf. [108]

OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264276284-en. [20]

OECD (2016), *Big data: Bringing competition policy to the digital era*, https://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm (accessed on 14 February 2020). [4]

OECD (2016), *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264255258-en. [163]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [3]

OECD (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264232440-en. [19]

OECD (2013), *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Publishing, http://dx.doi.org/10.1787/20716826. [18]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [11]

OFT (2012), *Anticipated acquisition by Facebook Inc of Instagram Inc*, https://webarchive.nationalarchives.gov.uk/20160815232112/https://assets.publishing.service.gov.uk/media/555de2e5ed915d7ae200003b/facebook.pdf. [78]

Ohlhausen, M. (2019), *Privacy and Competition: Friends, Foes, or Frenemies?*, Competition Policy International, pp. 14-18, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf. [88]

Ohlhausen, M. and A. Okuliar (2015), "Competition, Consumer Protection, and the Right [Approach] to Privacy", *Antitrust Law Journal*, Vol. 80/1, pp. 121-156, https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf. [164]

Open Banking (n.d.), *Open Banking*, https://www.openbanking.org.uk/. [34]

Park, M. (2011), "The Economic Impact of Wireless Number Portability", *The Journal of Industrial Economics*, Vol. 59/4, pp. 714-745, https://onlinelibrary.wiley.com/doi/full/10.1111/j.1467-6451.2011.00471.x. [142]

PCAST (2014), *Big Data and Privacy: A Technological Perspective*. [24]

Pecman, J., P. Johnson and J. Reisler (2020), *Essential facilities fallacy: Big tech, winner-take-all markets, and anticompetitive effects*, Competition Policy International, p. 21, https://www.competitionpolicyinternational.com/wp-content/uploads/2020/02/AC-February-II.pdf. [57]

Petit, N. (2019), *Are "FANGs" Monopolies? A Theory of Competition Under Uncertainty*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3414386. [186]

Picker, R. (2008), "Competition and Privacy in Web 2.0 and the Cloud", *Northwestern University Law Review Colloquy*, Vol. 103/1, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1147&context=journal_articles. [135]

Posner, E. and E. Weyl (2019), *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*, Princeton University Press. [157]

Preibusch, S., D. Kübler and A. Beresford (2013), "Price versus privacy: an experiment into the competitive advantage of collecting less personal information", *Electronic Commerce Research*, Vol. 13, pp. 423–455, https://link.springer.com/article/10.1007/s10660-013-9130-3. [120]

Productivity Commission (2017), *Data Availability and Use*, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf. [182]

Purra, J. and N. Carlsson (2016), *Third-Party Tracking on the Web: A Swedish Perspective*, http://dx.doi.org/10.1109/LCN.2016.14. [48]

PwC (2017), *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html. [131]

Rich, J. (2014), *Letter to Facebook and WhatsApp*, https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf. [84]

Robertson, V. (2020), "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", *Common Market Law Review*, Vol. 57, pp. 161–189, https://ssrn.com/abstract=3408971. [16]

RSA (2019), *RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses*, https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf. [114]

Rubinfeld, D. and M. Gal (2017), *Access Barriers to Big Data*, p. 339, https://arizonalawreview.org/pdf/59-2/59arizlrev339.pdf. [37]

Ryte (2019), *Tracking Pixel*, https://en.ryte.com/wiki/Tracking_Pixel#What_is_a_tracking_pixel.3F. [46]

Solove, D. (2013), "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review*, Vol. 126, pp. 1880-1903, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018. [181]

Srinivasan, D. (2019), "The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy", *Berkeley Business Law Journal*, Vol. 16/1, p. 39, https://lawcat.berkeley.edu/record/1128876?ln=en. [124]

Statistica (2020), *Internet of Things - number of connected devices worldwide 2015-2025*, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [22]

Stauber, P. (2019), *Facebook's Abuse Investigation in Germany and Some Thoughts on Cooperation Between Antitrust and Data Protection Authorities*, Competition Policy International, pp. 36-43, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf. [176]

Stigler Committee (2019), *Stigler Committee on Digital Platforms, Final Report*, https://research.chicagobooth.edu/stigler/media/news/committee-on-digitalplatforms-final-report. [172]

Stucke, M. (2018), *Should We Be Concerned About Data-opolies?*, p. 275, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144045. [66]

Stucke, M. and A. Grunes (2016), *Big Data and Competition Policy*, Oxford University Press. [25]

Swire, P. and Y. Lagos (2013), "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique", *Maryland Law Review*, Vol. 72/3, pp. 335-380, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2159157. [139]

Thompson, W., H. Li and A. Bolen (n.d.), *Artificial intelligence, machine learning, deep learning and beyond: Understanding AI technologies and how they lead to smart applications*, https://www.sas.com/en_us/insights/articles/big-data/artificial-intelligence-machine-learning-deep-learning-and-beyond.html. [54]

Tide (2019), *The Personal Data Economy: Technical Whitepaper*, https://tide.org/Tide_Whitepaper.pdf. [156]

Trustpilot (2018), *Open Banking expected to contribute over £1 Billion annually to UK economy supporting 17,000 new jobs*, http://press.trustpilot.com/news/2018/2/26/open-banking-expected-to-contribute-over-1-billion-annually-to-uk-economy-supporting-17000-new-jobs. [145]

Turow, J. (2017), *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*, Yale University Press. [38]

Turow, J. (2003), *Americans Online Privacy: The System Is Broken*, The Annenberg Public Policy Center of the University of Pennsylvania, http://repository.upenn.edu/asc_papers (accessed on 8 August 2017). [183]

Turow, J. et al. (2009), "Americans Reject Tailored Advertising and Three Activities That Enable It", Vol. 9, http://dx.doi.org/10.2139/ssrn.1478214. [184]

UIDAI (n.d.), *About UIDAI*, https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html. [159]

United States Department of Energy (n.d.), *Green Button: Open Energy Data*, https://www.energy.gov/data/green-button. [32]

United States v. Bazaarvoice (2014), *Competitive Impact Statement*, https://www.justice.gov/atr/case-document/file/488826/download. [87]

Waehrer, K. (2016), *Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions*, http://dx.doi.org/10.2139/ssrn.2701927. [123]

Walters, R., B. Zeller and L. Trakman (2018), *Personal Data Law and Competition Law - Where is it Heading?*, pp. 18-73, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275832. [115]

Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs. [39]