

Consumer data and competition: A new balancing act for online markets?



This Toolkit note was written by Anna Barker. It was reviewed and approved by the Competition Committee on 18 December 2020. The note was prepared for publication by the OECD Secretariat.

This Toolkit note is a contribution to the OECD Going Digital project, which aims to provide policy makers with the tools they need to help their economies and societies thrive in an increasingly digital and data-driven world.

For more information, visit www.oecd.org/going-digital.

#GoingDigital

Please cite this publication as:

Barker, A. (2021), "Consumer data and competition: A new balancing act for online markets?", *Going Digital Toolkit Note*, No. 5, https://goingdigital.oecd.org/data/notes/No5_ToolkitNote_ConsumerData.pdf.

Note to Delegations:

This document is also available on O.N.E. under the reference code:

DAF/COMP(2020)18/FINAL.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

© OECD 2021

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for commercial use and translation rights should be submitted to: rights@oecd.org.

Table of Contents

Consumer data and competition: A new balancing act for online markets?	4
How and why businesses use consumer data.....	6
Competition enforcement and consumer data.....	8
Analytical challenges.....	11
Potential remedies	13
Co-operation across policy areas and borders.....	15
Annex. A selection of case studies on consumer data and competition	15
References	17

Tables

Table 1. Barriers to entry in the data supply chain	11
---	----

Boxes

Box 1. What are consumer data?.....	5
Box 2. Online tracking technologies	7

Consumer data and competition: A new balancing act for online markets?

The impact of consumer data on competition in online markets is gaining attention from competition agencies across the globe. Effective competition should theoretically drive better outcomes for consumers in terms of higher levels of privacy and control of personal data, but this is not always the case in practice, especially when consumers do not or cannot actively manage their privacy options. There are questions about whether the possession of consumer data raises barriers to entry and what remedies could best address such concerns, among others. This Going Digital Toolkit note discusses competition issues and identifies innovative ways that competition agencies are addressing related challenges. It also assesses some of the ways in which jurisdictions are improving co-operation between agencies with responsibilities across competition, privacy and data protection, and consumer policy and enforcement.

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 ... are traded and used across sectors and national borders”* (OECD, 2015^[3]).

A range of businesses now rely on the consumer data that they collect as consumers use the Internet, digital applications (apps) and connected devices. In this context, the analysis and use of consumer data has brought a wide range of new and innovative goods, services and business models, often at a zero (monetary) price. 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 harm consumers. In response, a number of OECD countries have recently enacted, or are considering enacting, new data protection and privacy laws to provide greater levels of privacy and consumer control of their data.

New business models based on the collection and use of consumer data raise new issues for competition policy (see Box 1 for a working definition of consumer data). For example, competition agencies may wish to assess whether businesses compete on privacy. Where a business responds to the level of privacy offered by competitors, or differentiates itself in respect of the level of privacy it offers, this could suggest that privacy is a relevant parameter of competition. In such cases, a key question for competition agencies is how to incorporate this into competition assessments? In addition, competition agencies may wish to consider when and in which circumstances consumer data might raise barriers to entry or expansion, and when consumer data might be an essential input for complementary, competing or downstream businesses. Further, competition agencies may want to consider how business and regulatory decisions regarding the collection, storage and use of consumer data affect competition and the broader economy.

Most OECD member countries have privacy and data protection legislation in place, consistent with the framework set out in the OECD Privacy Guidelines (OECD, 2013^[4]), which is currently under review. 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 at least a partial consent-based regime, which provides consumers the ability to control how personal data are collected and used by agreeing or withholding consent. Jurisdictions have also enacted provisions that ensure that data are only collected and used by lawful and fair means. In some jurisdictions, privacy and data protection legislation also 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; and
- The right to data portability, which provides data subjects the ability to transfer their personal data from one data controller to another (OECD, 2020^[5]).

Box 1. What are consumer data?

The term “consumer data” is intended to capture data concerning individual consumers, where such data have been collected, traded or used as part of a commercial relationship (including for zero-priced digital services). That is, consumer data is “any information related to an identified or identifiable consumer” (OECD, 2019^[7]).

This is in some ways narrower than the concept of “personal data”, which is defined in the OECD’s Privacy Guidelines as “any information relating to an identified or identifiable individual (data subject)” (OECD, 2013^[4]). That is, “personal data” tends to encompass an individual’s data, irrespective of whether the individual acts as a consumer, citizen or otherwise. However, the concept of consumer data used in this paper applies only to personal 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.

The term “consumer data” is also broader than “personal data” since it may also capture data concerning consumers even where the data no longer relates to an identified or identifiable individual (i.e. non-personal data). For example, anonymised data about consumers (i.e. data that businesses might use to train artificial intelligence (AI) systems, for example) may be consumer data but not personal data. 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. That said, the increasing ability of data analytics and AI to help re-identify individuals based on anonymised data makes the distinction between personal data and consumer data increasingly blurry.

As noted in OECD (2019^[7]), consumer data could include, for example:

- User generated content, including blogs and commentary, photos or videos;
- Activity or behavioural data, including what people search for and look at on the Internet, what people buy online, as well as how much and how they pay;
- Social data, including contacts and friends on social networking sites;

- Locational data, including residential addresses, GPS and geo-location (e.g. from cellular mobile phones), or IP addresses;
- Demographic data, including age, gender, race, income, sexual preference, and political affiliation; and
- Identifying data of an official nature, including name, financial information and account numbers, health information, national health or social security numbers, and police records.

The collection and use of consumer data by businesses is also relevant to consumer protection and in many jurisdictions subject to consumer law (for example, where deceptive representations about consumer data practices, misrepresentations by omission or unfair consumer data practices are concerned). This is highlighted in the OECD's Recommendation on Consumer Protection in E-commerce (OECD, 2016^[8]) and the OECD Good Practice Guide on Consumer Data (OECD, 2019^[7]).

How and why businesses use consumer data

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 from its core business (Rubinfeld and Gal, 2017^[9]). 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. It took time, for example, for retail businesses to understand the value of retail scanner data (Turow, 2017^[10]). However, once retail businesses understood this value, many created fidelity or loyalty schemes to collect such consumer data. 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 underpinning its digital advertising activities (Zuboff, 2019^[11]). In many cases, once businesses start to understand the value of data, they move from passive to more active data collection practices.

When talking about the collection of consumer data, it is useful to distinguish between first- and third-party data. 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. In comparison, third-party data collection occurs when businesses collect consumer data from unaffiliated websites and apps, usually through third-party tracking (Robertson, 2020^[12]). 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). Online tracking is facilitated through a range of different technologies (Box 2), and third-party tracking is prevalent across websites and apps (Binns et al., 2018^[13]; Purra and Carlsson, 2016^[14]). However, the majority of tracking technologies are controlled by just a few businesses (Ezrahi and Robertson, 2019^[15]).

Box 2. Online tracking technologies

Traditionally, “cookies” (a text file with data that identifies a user’s computer and records certain user behaviour) were used to track online behaviour via desktop browsers. First-party cookies originate from (or are sent to) the website the consumer is viewing, whereas third-party cookies originate from (or are sent to) an unrelated website. Cookies are less effective at tracking online activity on mobile devices as they are not necessarily shared between apps, and some mobile browsers block third-party cookies by default.

As consumers now use a range of devices to access online services, businesses are using other means to track individuals online. These methods are often categorised as “deterministic” or “probabilistic”. Deterministic methods use consumer identifying characteristics, such as a log-ins, to track consumers across devices. Probabilistic methods instead infer a consumer’s identity through means such as IP address; geolocation information; browser or device fingerprinting; and general usage patterns.

In addition, businesses are increasingly using tracking pixels to facilitate third-party tracking. Pixels are small (essentially invisible to the naked eye) 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.

Source: Adapted from OECD (2020[5]), and referencing Beal (2008[16]); IAB (2013[17]); FTC (2017[18]); Boerman et al. (2017[19]); OECD (2019[20]); Ryte (2019[21]).

How a business collects consumer data can affect competition outcomes in markets. In particular, a business’ ability to recreate or otherwise access similar consumer data as held by a competitor will 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 precursor to effective competition. That is, even when 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.

Business decisions regarding how and where data is stored may influence privacy and competition outcomes. For example, whether personal data collected from a connected device is stored on the device or externally (e.g. with the manufacturer or in the cloud) will affect privacy and competition outcomes (Kerber, 2019^[22]).¹ Data that is stored locally on a consumer’s device, that is inaccessible by any other parties without explicit consent, is less likely to raise privacy concerns. However,

¹ The consumer privacy and security-related risks of smart home devices are discussed in detail in OECD (2018^[113]).

benefits that could potentially arise from broader analysis and use of this data may not be realised. Alternatively, data held by the manufacturer or in the cloud has more potential to raise privacy concerns. If businesses do not share such data more broadly, this may limit the benefits that could arise from widespread use of the data.

Declining costs of data storage and processing have facilitated more affordable data analytics, especially through cloud computing (OECD, 2015^[23]). 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; and
- Sell advertising products or services.

In addition, businesses can sell consumer data, including personal data, to third parties (potentially subject to consumer approval or anonymisation, depending on the regulatory regime in place) (Gilbert and Pepper, 2015^[24]). 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^[25]).

Given these various uses, consumer data can have substantial economic value, which provides an incentive for businesses to collect ever-greater volumes of data. There also appears to be a feedback loop between a business' 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^[27]).

Of course, the use and analysis of consumer data is not costless, and at some point the marginal costs of additional collection and use of consumer data may exceed its marginal benefits to businesses. In particular, there are computing and storage costs as well as staff costs associated with using and analysing consumer data. Indeed, many have argued that the value in consumer data lies not in the data itself, but in combining data and using algorithms and other analytics to glean insights (Körber, 2018^[28]). In this way, Lambretch and Tucker (2017^[29]) argue that it is access to skilled labour, rather than raw data (which they find is usually easy to replicate), that gives businesses a competitive advantage.

Competition enforcement and consumer data

While businesses have collected and used consumer data for a long time, this has grown exponentially recently. This means that consumer data is increasingly relevant to competition assessments. This can manifest in two key ways: 1) privacy

and data protection might be an aspect of quality on which businesses may compete; and 2) the collection and ownership of consumer data, and access to that data, might impact competition.

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 with greater co-operation between data protection, competition law and consumer protection (EDPS, 2014^[30]). It highlighted issues associated with zero-price markets in which consumers “pay” with their data, and the impacts of privacy on consumer welfare.² Similarly, in 2015 the UK’s Competition and Markets Authority (CMA) published a report on the commercial use of consumer data, which looked at some of the interactions between competition and privacy, including potential demand-side barriers to better privacy outcomes (CMA, 2015^[25]). These issues were also touched on in the OECD’s 2016 hearing on “Big Data” (OECD, 2016^[31]). A joint report between the German and French competition authorities, also in 2016, considered the interplay between competition law and data.

Privacy as an aspect of competition was also discussed in the OECD’s 2018 background paper on quality considerations in the zero-price economy (OECD, 2018^[32]). Further, the UK’s 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^[33]). There are still few cases where issues related to privacy or consumer data have been determinative, as will be discussed below. Nonetheless, there appears to be growing acceptance that these issues may be relevant to competition assessments (OECD, 2016^[31]; OECD, 2018^[32]; OECD, 2018^[34]; Robertson, 2020^[12]; Kemp, 2019^[35]).

Consumer data, privacy and mergers

Mergers between businesses that use consumer data could potentially harm competition in two ways: 1) by reducing the quality of data protection and privacy on offer in the relevant market, or 2) by raising barriers to entry or raising rivals’ costs through the merging of consumer data. Concerns about mergers reducing competition in respect of privacy might be especially relevant in zero-price markets where competition is largely on elements of quality rather than price (OECD, 2018^[32]). Further, Gilbert and Pepper (2015, p. 5^[24]) 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.

There seems to be growing acceptance that privacy may be relevant to merger assessments where the relevant businesses compete on privacy (and consumers

² Indeed the OECD E-Commerce Recommendation (which was revised in 2016) now explicitly includes non-monetary transactions in its scope (OECD, 2016^[8]).

value this competition). That said, to date there do not appear to be any mergers that competition authorities have blocked due to these concerns alone.

Mergers could also raise concerns when the merging of consumer data has the potential to raise barriers to entry or raise rivals' costs. However, in assessing the potential impact of mergers in this context, competition agencies should also consider any potential efficiency benefits that arise in tandem (according to the relevant standards and tests in their jurisdiction). In cases where competition agencies find the merging of consumer data has an anticompetitive impact, a potential remedy could be to require the merged party to grant competitors access to its merged dataset on a fair, reasonable and non-discriminatory (FRAND) basis (OECD, 2020^[5]; Crémer, de Montjoye and Schweitzer, 2019^[36]).

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. For example, in allowing a merger between Ticketmaster and Live Nation, both operators in the market for primary ticketing of major concert venues, the U.S. Department of Justice required that the merged party provide ticketing clients with their ticketing data in a reasonably usable form upon request (DOJ, 2010^[37]). That is, it required data portability (Jones Harbour and Koslov, 2010^[38]).

Abuse of dominance

In theory, a dominant firm could abuse its dominance by lowering the level of privacy and data protection it offers to consumers (Kemp, 2019^[35]; Ezrachi and Roberston, 2019^[15]). This could arguably constitute an exploitative abuse in some jurisdictions. For example, Stucke (2018, pp. 285-286^[39]) argues that a dominant business:

...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^[15]).

In practice, there are few examples of these types of cases. One recent example is the German Competition Authority's (GCA) case against Facebook. In February 2019, the GCA found that Facebook had abused its dominant position in the social media market in respect of the collection of "off Facebook" data (OECD, 2020^[40]). That is, data collected from unrelated third parties to support Facebook's online advertising services (Bundeskartellamt, 2019^[41]). It argued that Facebook's dominant market position essentially put consumers in a "take-it-or-leave-it" position and Facebook's data practices served to entrench Facebook's dominant position in the national social network market (Bundeskartellamt, 2019^[41]). Facebook appealed the decision to the Higher Regional Court in Dusseldorf, who suspended the order in August 2019 (ruling in Facebook's favour on substantive grounds regarding whether the practice in

question was a source of competition harm). The GCA appealed the suspension to the Federal Court of Justice (the BGH), who in interim proceedings on 23 June 2020 regarding enforceability, ruled in favour of the GCA (Podszun, 2020^[42]). The case is ongoing and pending a decision by the Düsseldorf Higher Regional Court on merits.

In addition, there is potential for a business to engage in exclusionary abuse of dominant practices. In particular, a dominant firm could restrict a competitor's access to consumer data to foreclose competitors or raise rivals' costs. There have been number of cases of this type. For example, in January 2018, the Competition Bureau of Canada (CBC) reached an agreement with Softvoyage, Inc. ("Softvoyage"), a provider of software for the travel industry, to remove exclusivity clauses in its agreements with customers that prevented those customers from extracting or using their own data from Softvoyage's software (OECD, 2020^[43]). Similarly, in December 2018, the Italian Competition Authority found that two electricity companies had abused their dominance in the regulated segment of the market to use consumer data to try and lock in consumers at the retail level in anticipation of the retail market being liberalised (OECD, 2020^[44]). 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.

Cartels and collusion

While no cases appear to have been introduced to date, collusion based on the level of privacy offered to consumers could 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. In addition, sharing of data between competitors can sometimes raise competition concerns. However, in practice, competition agencies have often allowed businesses to share (certain) consumer data, either because it is not expected to have an anti-competitive effect, or because it could be expected to foster competition.

Analytical challenges

In assessing the impacts of consumer data on competition, there are a number of analytical challenges.

Barriers to entry

Several characteristics of online 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^[35]). Where these characteristics necessitate a business to incur substantial sunk costs to enter the relevant market, they could represent barriers to entry. Rubinfeld and Gal (2017^[9]) 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 (Table 1).

Table 1. Barriers to entry in the data supply chain

	Technical barriers	Legal Barriers	Behavioural barriers
Collection	<ul style="list-style-type: none"> • Uniqueness of the data, or access to it • Supply side: economies of scale, scope, learning by doing, speed • Demand side: network effects and two-sided markets 	<ul style="list-style-type: none"> • Data protection and privacy laws • Data ownership 	<ul style="list-style-type: none"> • Exclusivity agreements • Access prices and conditions • Disabling data collecting software
Storage	<ul style="list-style-type: none"> • Storage costs 	<ul style="list-style-type: none"> • Data protection and privacy laws 	<ul style="list-style-type: none"> • Lock-in and switching costs
Synthesis and analysis	<ul style="list-style-type: none"> • Lack of data interoperability (including a lack of standardisation) • Analytical tools 		
Use	<ul style="list-style-type: none"> • Inability to locate and reach relevant consumers • Lack of data interoperability (including a lack of standardisation) 	<ul style="list-style-type: none"> • Data protection and privacy laws • Antidiscrimination laws 	<ul style="list-style-type: none"> • Contractual limitations

Source: Rubinfeld and Gal (2017^[9]); Gal and Rubinfeld (2019^[26]); CMA (2016^[45]).

Do consumers value privacy?

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^[46]). While attitudes to privacy vary between individuals and regions depending on a number of factors, numerous surveys have shown that consumers value privacy and are increasingly concerned about their privacy online (Cisco, 2019^[47]; Auxier et al., 2019^[48]; RSA, 2019^[49]). However, in the context of a competition assessment, it can be difficult to understand the importance of privacy and data protection in the specific market(s) under investigation.

Consumer attitudes regarding privacy are “subjective and idiosyncratic” (Acquisti, Taylor and Wagman, 2016, p. 446^[50]). Consumers tend to have heterogeneous preferences for privacy (Walters, Zeller and Trakman, 2018^[51]) and the decision about whether to share or withhold personal information will depend on the context in which the information is requested as well as cultural and other factors (Acquisti, Taylor and Wagman, 2016^[50]; OECD, 2019^[52]).

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^[50]). This can be particularly problematic given that consumers tend to be myopic and subject to time inconsistent preferences (Choi,

Jeon and Kim, 2019^[53]), not to mention that many consumers are time constrained. The way in which privacy options are presented can also lead to greater collection of data given that consumers tend to stick with default privacy settings due to the *status quo* bias (Costa-Cabral and Lynskey, 2017^[54]). 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^[32]).

Some 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^[55]; Costa-Cabral and Lynskey, 2017^[54]). Such concerns may reflect a lack of effective competition in the market. Alternatively, the inability of consumers to engage with privacy policies (and behavioural biases limiting their ability to engage with privacy policies) may result in consumers agreeing to practices they do not condone (OECD, 2019^[7]; OECD, 2018^[56]). In this respect, there have been serious concerns raised about consumers’ ability to understand and act on privacy notices (Hoofnagle and Whittington, 2014^[57]). These issues can manifest in the so-called “privacy paradox” whereby 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^[58]; Kokolakis, 2017^[59]; OECD, 2018^[32]).

As noted by the CMA (2015^[25]), 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 the data, and the value of the data, they may not be in a position to make informed decisions with privacy in mind. Hence, businesses may have limited incentives to compete on privacy (Farrell, 2012^[60]; Lynskey, 2018^[61]). 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^[54]; Lynskey, 2018^[61]). Taken together, these issues can make it difficult to understand in which circumstances and markets consumers actually understand and value privacy, both in theory and in practice.

In cases in which privacy appears to be a relevant consideration, competition agencies could potentially undertake consumer surveys to better understand consumer views regarding privacy in the particular case under investigation. For example, in assessing a merger, it might be useful to understand whether any apparent differences in the level of privacy offered by the merging parties are important to consumers. For an abuse of dominance case, it might be useful to understand whether consumers are satisfied with the level of privacy offered, and if not, why not.

Such surveys could be undertaken in co-operation with data protection authorities, who routinely undertake such surveys. However, such surveys are costly and time consuming, meaning they should only be undertaken when privacy appears to be a key aspect of competition in the relevant market. 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 the relevant market.

Do businesses compete on privacy?

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 claiming a reduction in privacy or excessive data collection, it will be important to assess the dominant business' privacy and data protection practices.

A number of sources of evidence 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, these surveys could include questions about whether privacy is an important aspect of competition in the relevant market, and whether it is something that consumers value. For example, in its consideration of the Microsoft/LinkedIn merger in 2016, the European Commission (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^[62]). The EC ultimately found that privacy is an important parameter of competition and driver of consumer choice in the market for professional social network services. The EC ultimately allowed the merger subject to a number of commitments; none of which addressed privacy specifically (European Commission, 2016^[63]).

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^[64]). For example, Jones Harbour and Koslov (2010^[38]) 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 it to three months. In addition, businesses' 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.

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 in assessing the effect of abusive conduct on consumers. For example, Srinivasan (2019^[65]) argues that recent degradations in privacy on social media networks are due to rising levels of market power leaving consumers no alternative option (at least none with a pre-installed user base).

Potential remedies

The types of remedies available to competition authorities depend on the theory of harm. Other policy responses may also be envisaged.

Competition policy responses

For **mergers**, 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 the merged entity to provide competitors with access to the data set under FRAND terms (Cr  mer, de Montjoye and Schweitzer, 2019^[36]), although the development of such terms may be particularly challenging. In such cases, it will be important to ensure that such remedies do not undermine other policy objectives, such as data protection and privacy.

In contrast, a structural remedy may require the merged entity to divest a dataset, where access to the dataset is important to competition.³ If the concern is that the merged entity will not have sufficient competitive pressure to offer competitive levels of privacy, a competition authority could consider blocking the merger (to the extent that allowing it would reduce consumer welfare). Of course, this is not necessarily straightforward to demonstrate, as discussed above.

In **abuse of dominance** cases, requiring the business to provide access to their consumer data may be appropriate when the competition concern involves access to a consumer dataset. For example, 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^[66]; Autorit   de la concurrence, 2014^[67]). In such cases, data protection and privacy concerns need to be considered. These can potentially be managed by allowing consumers to opt-in or opt-out of their data being made available to other businesses. Remedies in cases concerning dominant players engaging in excessive consumer data collection, use and/or sharing, however, may be more difficult. In particular, it will be difficult to determine what level of data protection would exist if there was more competition in the relevant market.

For **cartels and collusion** involving the anticompetitive sharing of consumer data, a behavioural remedy requiring parties to stop sharing the relevant data might address the competition concern. Competition agencies could also consider issuing guidance on the types of data that are more or less likely to raise competition concerns.

³ More generally, Line of Business Restrictions (LOBRs) were discussed as part of the Competition Committee's Working Party 2 discussions in June 2020. See: <http://www.oecd.org/daf/competition/line-of-business-restrictions-as-a-solution-to-competition-concerns.htm>.

One advantage of using competition law to facilitate the movement of data between businesses (rather than explicit data portability requirements, which generally apply to consumer data that an individual consumer decides to take with them to a new service or platform) is that competition law can apply to all types of data (Graef, Verschakelen and Valcke, 2013^[68]; Engels, 2016^[69]). Further, as competition law remedies can be more targeted to the specific competition issue under consideration, they only impose compliance costs in cases where there is (or is expected to be) an identified competition concern.

Competition law remedies are also more flexible than ex ante legislation, in that they can adjust to the requirements of the specific market under investigation. 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 often difficult to generalise. To this end, targeted but systematic data portability requirements may be more beneficial in circumstances where there has been an identified market or policy failure which those requirements can address, rather than relying on more ad hoc ex post enforcement of competition law.

Another possible solution under competition law is to consider whether the essential facilities doctrine (EFD) applies. Under the EFD doctrine, many OECD jurisdictions allow a business to seek access to another business' assets if access is necessary to provide another good or service. The EFD 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. However, some experts have raised the question of whether data could be an "essential facility" to which the essential facilities doctrine could potentially apply, with some lending support to the idea (Crémer, de Montjoye and Schweitzer, 2019^[36]; Diker Vanberg and Ünver, 2017^[70]; Haucap, 2019^[71]), and others arguing against using the EFD to provide access to data (Körber, 2018^[28]; Lambretch and Tucker, 2017^[29]; Gilbert and Pepper, 2015^[24]).

Other policy responses

In some cases, certain issues associated with consumer data may be better addressed through other policy instruments, such as direct privacy regulation. Similarly, there could be a case for mandating greater consumer control of data through sector-specific or economy-wide regulations such as to promote data portability or greater data interoperability. Of course, the costs and benefits of such policies, including on competition in relevant markets, should be carefully weighed before their introduction, and monitored post-introduction to ensure the intended benefits are achieved and outweigh any associated costs. In other cases,

the role may be for consumer law enforcement to ensure that consumers are not misled regarding how a business collects and uses their personal information.

Co-operation across policy areas and borders

As outlined in the Going Digital Integrated Policy Framework, digital transformation has widespread and complex effects across policy domains (OECD, 2020^[72]). The use of consumer data by businesses raises issues across multiple policy areas and the intersection of these areas is difficult to navigate. For example:

- The way that privacy and data protection (and potentially consumer) policies are drafted and implemented has the potential to affect competitive outcomes in markets subject to those policies.⁴
- Some forms of business conduct that may raise competition concerns (for example, a dominant firm refusing to share consumer data with competing or downstream businesses) may be defended by the business on the grounds of protecting consumer privacy.
- Remedies under one policy area have the potential to affect outcomes in other policy areas (for example, a competition remedy that requires data sharing could have implications for privacy and liability).
- Certain forms of conduct could arguably be contrary to competition, consumer and data protection laws. For example, in some jurisdictions consumer protection cases have been taken against certain platforms in respect of their data practices (see OECD (2019^[71]), whereas in other jurisdictions this has been taken under competition law.⁵ In some circumstances, such conduct could also be contrary to privacy and data protection laws.
- Understanding consumer behaviour is particularly relevant to cases involving consumer data, and may be an area where consumer and data protection agencies have more experience and knowledge than competition agencies.

For these reasons, there is a need for increasing co-operation across the policy areas of competition, consumer protection and privacy and data protection. The need for co-operation and co-ordination across agencies when issues span multiple policy domains has been discussed in multiple OECD reports (OECD, 2018^[32]; OECD, 2020^[73]; OECD, 2020^[72]; OECD, 2019^[52]; OECD, 2018^[74]; OECD, 2019^[75]; OECD,

⁴ See, for example, concerns about the competition impacts of Europe's General Data Protection Right (GDPR) are discussed in Swire and Lagos (2013^[111]), Diker Vanberg and Ünver (2017^[70]) and Gal and Aviv (2020^[112]).

⁵ For example, the German competition authority has taken an abuse of dominance case against Facebook in relation to its data practices (see Annex A), whereas similar conduct has been investigated or tried as a breach of consumer laws in Italy and the United States (see Annex A as well as Box 12 in OECD (2020, p. 48^[73])).

2015^[3]). This has also been discussed by data protection agencies, who have supported 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 (EDPS, 2014^[30]; EDPS, 2016^[76]).

The co-ordination of competition and consumer policy issues and enforcement is generally more straightforward in more than 30 jurisdictions that have these responsibilities tasked to one common agency (Kovacic and Hyman, 2013^[77]). In addition, legislative provisions can provide the legal basis for co-operation between these authorities, as is the case in Germany (Stauber, 2019^[78]). Less formal means of co-operating are also available. For example, in 2016 the European Data Protection Supervisor recommended that a “Digital Clearinghouse” be created to facilitate information sharing between regulators relating to possible violations in online markets (EDPS, 2016^[76]). It was created through a 2017 Resolution of the European Parliament and brings together regulators across a range of policy areas both from within the European Union, as well as internationally (European Parliament, 2017^[79]).

A number of recent reviews of competition issues have recommended a new “digital regulator” of some form or another to look at competition and other issues that arise in relation to online platforms (ACCC, 2019^[80]; Furman et al., 2019^[33]; Stigler Committee, 2019^[81]). A Digital Platforms Branch has since been set up in Australia, as part of the Australian Competition and Consumer Commission (ACCC, n.d.^[82]) and a Digital Platforms Taskforce has been assembled in the United Kingdom (UK Government, 2020^[83]). The UK taskforce provides a particularly interesting example of how to address cross-cutting policy issues, by bringing together expertise from various agencies into one unit. The taskforce is housed within the CMA, headed by a senior CMA official, and comprises staff from the CMA, the Office of Communications (Ofcom), and the Information Commissioner’s Office (ICO) (UK Government, 2020^[83]). In addition, these three agencies have at various times signed Memorandum of Understanding to guide their working arrangements (UK Government, 2015^[84]; Ofcom, 2016^[85]; ICO, 2019^[86]).

In addition, given that consumer data can travel across international borders in online markets, international co-operation and co-ordination are required. As far as international co-operation between competition authorities goes, initiatives such as the Multilateral Mutual Assistance and Cooperation Framework for Competition Authorities that has recently been signed between competition agencies in Australia, Canada, New Zealand, the United Kingdom and the United States, provide a framework for such co-operation (FTC, 2020^[87]). The OECD is currently undertaking joint work with the International Competition Network to identify current barriers to co-operation, and potential ways to improve international co-operation. Similar work has been undertaken in respect of improving international co-operation between agencies in respect of consumer law enforcement (see, for example, OECD (2018^[88])) and privacy enforcement (see, for example, OECD (2007^[89])). International forums such as the OECD also allow for best practice ideas to be shared both between jurisdictions and across policy areas.

Annex. A selection of case studies on consumer data and competition

This annex presents case studies that highlight how competition authorities are considering consumer data and competition in practice.⁶

Guidance materials

Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information

Responsible entity: The Japan Fair Trade Commission (JFTC)

Description: In recognising the growing role of consumer data, the JFTC established a study group and conducted interviews to explore if and how the Japanese anti-monopoly act (AMA) could be applied to abusive behaviours by digital platforms regarding the use of personal information (OECD, 2020_[90]). Based on this, the JFTC published new guidelines in 2019 that clarify when it might consider the acquisition, possession or use of personal information by digital platforms to be an abuse of a superior bargaining position (ASBP) under the AMA. The guidelines point out that if an online platform disadvantages or hurts consumers by abusing a severe bargaining position, such conduct will not only impede the free and independent choice of consumers, but it will also likely give the online platform an advantage over its competitors. The guidelines also provide several examples of unjustifiable acquisition or use of consumers' personal information that may constitute an ASBP. For example, if a digital platform acquired information beyond the scope necessary to achieve the original stated purpose of use without obtaining the consent of consumers, or by compelling consumers to consent.

Read more: <https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217DPconsumerGL.pdf>.

Competition cases involving privacy

German case against Facebook

Responsible entity: The German Competition Authority (GCA), Bundeskartellamt

Description: In February 2019, the German Competition Authority (GCA) found that Facebook had abused its dominant position in the social media market in respect of the collection of “off Facebook” data (OECD, 2020_[40]). That is, data collected from unrelated third parties. Such data was used to support Facebook's

⁶ These examples draw on the country contributions submitted in relation to the OECD's June 2020 roundtable on consumer data rights and competition (OECD, 2020_[73]).

online advertising services, which contributed 98% of Facebook's revenue in 2018 (Bundeskartellamt, 2019^[41]).

The GCA found that Facebook was dominant in the social media market in Germany and that it had not gained meaningful consent from users in respect of its data tracking practices, and the merging of this data to users' Facebook profiles (Bundeskartellamt, 2019^[41]). In assessing Facebook's data practices, the GCA applied the standards in the GDPR and found Facebook's practices lacking, which it found amounted to an abuse of dominance (Bundeskartellamt, 2019^[41]). It argued that Facebook's dominant market position essentially put consumers in a "take-it-or-leave-it" position and Facebook's data practices served to entrench Facebook's dominant position in the national social network market (Bundeskartellamt, 2019^[41]).

Facebook appealed the decision to the Higher Regional Court in Dusseldorf, who suspended the order in August 2019 (ruling in Facebook's favour). The GCA appealed the suspension to the Federal Court of Justice (the BGH). In its decision on interim proceedings on 23 June 2020 regarding enforceability, the BGH ruled in favour of the GCA (Podszun, 2020^[42]). It found there were no serious doubts as to Facebook's dominant position nor Facebook's abuse of this position by using the terms of service prohibited by the GCA (Podszun, 2020^[42]). The BGH found that the terms of service deprive Facebook users of choice, and that this could impede competition, both in social network markets, and potentially, digital advertising markets (Podszun, 2020^[42]). However, the BGH did not agree with the GCA's approach to using the GDPR as the relevant standard for assessing an abuse of dominance (Podszun, 2020^[42]). The case is ongoing and pending a decision by the Düsseldorf Higher Regional Court on the merits.

Read more: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

Competition cases involving access to consumer data

Financial sector cases in Brazil

Responsible entity: CADE (Brazil's Administrative Council for Economic Defence)

Description: CADE has an ongoing investigation into the financial sector (OECD, 2020^[91]). The collection and use of consumer data is essential to the financial sector and facilitates efficiency by allowing firms to set rates according to their assessment of a consumer's risk. In this respect, larger banks may have an advantage over smaller banks, which may be problematic given low switching rates in the sector. With the emergence of fintech businesses, customers can extract more value from their data if they are able to share that data.

In this respect, CADE is currently investigating whether Bradesco, one of the largest Brazilian retail banks, hindered the development of the Brazilian fintech, Guiabolso, which could potentially harm not only the company itself but also Brazilian customers of banking services generally. Guiabolso is a fintech that provides

personal finance management services by connecting consumers with credit institutions depending on the consumer's needs and financial history. To do so, it requests consent from its consumers to access their financial information held by various financial institutions. The concern was that Bradesco was not allowing Guiabolso customers to access their financial information held by Bradesco. Bradesco claimed this was due to privacy concerns. CADE is still investigating the case but is sceptical about whether privacy is a legitimate reason for blocking access where consumers are able to provide their consent to have their information shared via technological means (OECD, 2020^[91]).

CADE also considered the role of consumer data in the financial sector in 2016 when it approved a joint venture between Banco do Brasil, Bradesco, Caixa Econômica Federal, Itaú, and Santander (the five largest retail banks in Brazil) to create a new credit bureau (OECD, 2020^[91]). CADE recognised the benefits of the joint venture, namely enabling greater sharing of this data could improve efficiencies in the sector in respect of credit rates in particular. However, there was a concern that allowing the joint venture could advantage the parties to the joint venture. Hence, the approval of the joint venture was conditioned upon certain conditions including:

- Development of an upstream information control (by the banks) and a downstream usage of that information (by credit bureaus) and
- Guarantees of non-discrimination for competing credit bureaus accessing credit information.

This ensured that other financial institutions would also be able to benefit from accessing this information.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)41/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)41/en/pdf).

Canadian cases

Responsible entity: Canada's Competition Bureau (CBC)

Description: Two relevant competition cases in Canada include:

- In May 2011, CBC brought an abuse of dominance case against the Toronto Real Estate Board ("TREB") (OECD, 2020^[43]). TREB had rules that restricted its members from broadly disclosing historical real estate sales data online. The CBC was concerned that these restrictions were contrary to the Competition Act. The Canadian Competition Tribunal agreed, finding that TREB's restrictions prevented greater access to new and innovative real estate services, more in-depth listing information, and innovative online analytical tools. The Tribunal ordered TREB to remove these restrictions, thereby allowing TREB's real estate agent members to publish historical real estate sales data online.
- In January 2018, the CBC reached an agreement with Softvoyage, Inc. ("Softvoyage") to end certain anticompetitive business practices (OECD, 2020^[43]). Softvoyage, a company engaged in the development of software for the travel industry, included exclusivity clauses in its agreements with

customers that prevented those customers from extracting or using their own data from Softvoyage's software.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)31/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)31/en/pdf).

Egyptian consideration of ride sharing merger

Responsible entity: Egyptian Competition Authority (ECA)

Description: The ECA required data remedies, including data portability, to address competition concerns raised by Uber's acquisition of Careem, which brought together the two largest ride-sharing platforms in the region (OECD, 2020_[92]). The ECA considered the concentration of the merged party's data sets as a major part of this transaction, especially in light of the scarcity of such data in Egypt. Such data is fundamental to Uber's business model, and that of rival ride-sharing businesses. Finding that data possession is becoming a competitive advantage and a barrier to entry, the ECA found that allowing for the concentration of data in one entity would cause significant harm to competition in the market. Absent remedies, the concentration of data would have rendered entry unlikely, which would have reduced consumer choice. The ECA saw data portability as a way for consumers to avoid possible lock-in and for other firms to enter the market and hence, compelled Uber to continue granting its riders access to their data by enabling them to download this data. Uber also committed to employ its best efforts to facilitate the interoperability of this data with other platforms, in order to allow consumers to transfer their data to alternative ride sharing service providers.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)43/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)43/en/pdf).

Relevant mergers in the European Union

Responsible entity: European Commission (EC)

Description: The EC has cleared various mergers (and joint ventures) involving the combining of consumer data sets, including (OECD, 2020_[93]):

- *Telefonica UK/Vodafone UK/Everything Everywhere* joint venture: In 2012, the EC considered whether the venture could foreclose competing providers of targeted advertising services. Ultimately, it found that the information available to the joint venture was also available to existing and new market players that were already using it to provide targeted advertising. Therefore, the joint venture would not foreclose competitors from accessing an essential input or negatively affect competition (especially as the joint venture would be constrained by data protection laws).
- *Verizon/Yahoo!*: The EC examined whether the combination of the datasets of the two firms would increase the merged entity's market power or create barriers to entry in the market for online advertising. The EC concluded that the data protection rules would limit the parties' ability to use the personal data that they collected across the merged entity. Additionally, there would continue to be a large amount of valuable Internet user data that were not

within the exclusive control of the merged entity. Finally, the parties were small market players in online advertising.

- *Apple/Shazam*: A potential concern was that Apple would gain access to “commercially sensitive data” of its music streaming rivals, thus putting its competitors at a competitive disadvantage. The EC concluded that while Apple could have the ability to use Shazam’s data in this way, it was unclear whether it had an incentive to do so. Further, Shazam’s data was not unique and did not offer a significant advantage to Apple post-acquisition.
- *Facebook/WhatsApp*: The EC analysed whether data concentration was likely to strengthen Facebook’s position in the online advertising market. It explicitly left privacy concerns to the remit of EU data protection laws. The EC cleared the merger noting that WhatsApp did not collect any user data that are valuable for advertising purposes and thus, the transaction would not have increased the amount of data potentially available to Facebook for advertising purposes.
- *Microsoft/LinkedIn*: The EC assessed whether the combination of Microsoft’s and LinkedIn’s datasets would increase the market power of the merged entity or raise barriers to entry. It noted that applicable data protection rules may limit Microsoft’s ability to use its users’ personal data. In any event, the EC dismissed these concerns because the parties did not make their data available to third parties for advertising purposes, the data was not unique, and the parties were small players in online advertising.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)40/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf).

Italian energy sector case

Responsible entity: The Italian Competition Authority (AGCM)

Description: In December 2018, the AGCM imposed a fine of EUR 93 million and EUR 16 million on Enel Group and Acea Group respectively, both major utilities in the energy sector, for a breach of Art. 102 of the Treaty on the Functioning of the European Union (TFEU) (OECD, 2020^[44]). In particular, it found that the parties had implemented an exclusionary strategy aimed at foreclosing new entrants in the retail market for domestic users, which was due to be fully liberalised in July 2019. In particular, the AGCM found that Enel and Acea abused their individual dominant positions (in the captive markets) by inducing their captive customer base to switch from the regulated market to the liberalised one by signing contracts with their retail subsidiaries. In particular, the two groups used the confidential and sensitive information gathered from their captive clients (by acquiring a “privacy” consent to be re-contacted for commercial purposes) for the sole benefit of their retail subsidiaries in the liberalised market. According to the AGCM, the purpose of this was to retain their captive clients by hindering their possibility to switch to a different supplier in the liberalised market, pre-empting the opening of the retail market.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)33/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)33/en/pdf).

Spain

Responsible authority: The Spanish Competition Authority, Comisión Nacional de los Mercados y la Competencia (CNMC)

Description: CNMC has considered the impact of access to consumer data in a number of cases (OECD, 2020^[94]):

- A financial aggregator (Fintonic) claimed that a bank (Caixabank) refused to give access to certain client data. CNMC found that Caixabank's grounds for denying access were legitimate to ensuring data protection and security against fraud. It also found that the data was not critical to Fintonic's business and that the data could otherwise be obtained. Hence, the CNMC dismissed the case.
- Health Market Research España, S.L. (HMR) claimed that IMS Health, S.A. (IMS) held contracts with distributors of pharmaceutical products that limited distributors' ability to share data with IMS's competitors. Given IMS's position in the market, in its preliminary assessment, the CNMC concluded that such behaviour could amount to an abuse of a dominant position. IMS committed to remove the contentious clauses and so the CNMC closed the case.
- The Schibsted/Milanuncios merger involved the acquisition of a platform specialised in classified ads by multinational firm Schibsted. Although the parties overlapped in a number of markets, potential anticompetitive effects were only identified regarding professional advertisers in the market for free access platforms for online motor classified advertisements. The merger was cleared with commitments that the merged entity would licence out this service as offered by Milanuncios.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)38/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)38/en/pdf).

Competition cases in Turkey

Responsible entity: The Turkish Competition Authority (TCA)

Description: The TCA has considered the role of personal data in various cases involving investigations, merger reviews and exemptions (OECD, 2020^[96]). Two examples include:

- The TCA conducted an in-depth Phase II review of the acquisition of Migros Ticaret AŞ (Migros), an important supermarket chain in the Turkish consumer goods retail sector by Anadolu Endüstri Holding AŞ (AEH), the holding company of the Anadolu Group (OECD, 2020^[96]). TCA's major concern was related to the beer market, as Anadolu Efes – a joint venture between the Anadolu Group and SabMiller OLC – held a dominant position in the Turkish beer market. TCA highlighted the fact that Migros had the most comprehensive retail consumer data in Turkey. It is also stated that if Anadolu Efes is provided with access to the CRM dataset of Migros, then it would earn a significant competitive advantage that could be used to exclude rivals by

strengthening its dominant position. AEH submitted a set of behavioural commitments for a period of three years to mitigate TCA's concerns. One of these commitments was that Migros will refrain from sharing any commercially sensitive information regarding Anadolu Efes's competitors in the beer market or consumers who prefer competing products. The TCA granted the transaction conditional approval.

- Another case involved the electricity supply and distribution market. This case involved CK and EnerjiSa, both electricity distribution companies, withholding strategic information from independent Authorized Supply Companies (ASCs). The TCA found that this hindered independent suppliers' activities and prevented consumers from choosing their own supplier. The main reason was that if the distribution company did not provide the data, it would not be possible for ASCs to otherwise obtain that information, and this information (which included information about customers' address, phone number and consumption habits) was important in order to contact new customers. Its decision the TCA has forbid vertically integrated ASCs to access the information within the body of their distribution companies.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)55/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)55/en/pdf).

United States cases

Responsible entities: The US Department of Justice (DOJ) and the Federal Trade Commission (FTC)

Description: There have been a number of cases involving access to consumer data in the United States (OECD, 2020_[97]). Some examples include:

- *United States v. Thomson Corp.*: The DOJ required the divestiture of three financial data sets that were used by investment managers, investment bankers, traders, corporate managers, and other institutional customers in making investment decisions and providing advice to their firms and clients. The data in question were investment fundamentals data, earnings estimates data, and aftermarket research reports. The DOJ concluded that the merger of Thompson Corp. and Reuters would have eliminated competition between the two companies and led to higher prices and reduced innovation for fundamentals data, earnings estimates data, and aftermarket research reports. The settlement required the merging parties to sell copies of specified data sets and required licensing of related intellectual property.
- *United States v. Google Inc.*: Google purchased ITA Software, Inc. (ITA), the leading vendor of software to search for, price, and display results for airline travel queries. The DOJ determined that the proposed transaction could harm competition for airfare comparison and booking websites and diminish effective competition among websites using ITA's software to compete against any airfare website that Google might introduce. Two competitive concerns relevant to this paper were that Google, through the purchase of

ITA would: (1) obtain access to competitors' proprietary data in order to compete with those competitors and (2) deny competitors access to ITA's pricing and shopping software. The final judgement therefore required the merging parties to establish an internal firewall to prevent the misappropriation of competitively sensitive data and to license ITA's software to airfare websites on commercially reasonable terms. Google also was required to continue to fund research and development of that software at least at levels similar to what ITA had invested in prior years and to further develop and offer ITA's next software.

- *United States v. CVS*: The DOJ required the merging parties to divest Aetna's individual Medicare Part D prescription drug plan business to resolve the competitive concerns of higher prices for Medicare beneficiaries and taxpayers and lower quality service caused by the elimination of head-to-head competition between CVS and Aetna. Because continuity is important to retaining customers, the DOJ required that this divestiture include historical data related to the divested plans and broker contracts. Both the retail pharmacy rates for various drugs and the broker commissions are negotiated on an annual basis and significant changes to either can cause disruption for consumers. By requiring the divestiture to include historical data, the DOJ provided the divestiture buyer with the opportunity to replicate the prior cost structure and avoid price increases.
- *CoreLogic, Inc.*: Data were both a product and a divestiture asset, and the scope of a historical database in particular was seen as a barrier to entry for would-be competitors. The FTC alleged that the proposed acquisition would substantially lessen competition in the market for national real estate assessor and recorder bulk data by merging two of only three firms licensing such data. This would increase the risk of anticompetitive co-ordination between the two remaining market participants and the risk that CoreLogic would unilaterally exercise market power and raise prices. The data in question comprised public information about individual real estate properties, including descriptive information, such as square footage and the number of bedrooms, and financial data, such as purchase price, mortgage terms, and lien details. The settlement required that CoreLogic license bulk data, as well as several ancillary data sets, to a third-party entrant, to enable it to compete.
- *Verisk/EagleView*: The FTC challenged the proposed merger based on innovation effects related to data quality and coverage, alleging that the merger would likely reduce competition and result in a virtual monopoly in the US market for rooftop aerial measurement products used by the insurance industry to assess property claims. Data were regarded as necessary inputs into a relevant product market, where the acquirer's position in an adjacent market provided it with a unique opportunity to overcome data-related entry barriers. Although the data in question were not paradigmatic of things ordinarily considered personal information, the aerial image libraries at issue were images of consumer homes (specifically,

the roofs and surrounding property), which were combined with insurance information.

- In allowing a merger between Ticketmaster and Live Nation, both operators in the market for primary ticketing of major concert venues, the US DOJ required that the merged party provide ticketing clients with their ticketing data in a reasonably usable form upon request (DOJ, 2010^[37]). That is, it required data portability (Jones Harbour and Koslov, 2010^[38]).

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)39/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)39/en/pdf).

Cases under consumer law

Australian case against Google under consumer law

Responsible entity: The Australian Competition and Consumer Commission (ACCC)

Description: The ACCC has recently launched Federal court proceedings against Google, alleging that it misled consumers in respect of the collection and use of their data for digital advertising (ACCC, 2020^[98]). In particular, the ACCC claims that Google: “misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers’ internet activity, for use by Google, including for targeted advertising”.

While the ACCC has competition and consumer enforcement powers, it has chosen to take this case against Google in respect of its consumer powers. The ACCC may have considered taking such a case under competition law enforcement, had it considered that Google’s conduct amounted to a misuse of market power, contrary to Australia’s competition laws. However, such a case would arguably have been more difficult to pursue. In this case, vesting competition and consumer enforcement powers with the one agency allows the agency greater flexibility to decide how to pursue a case when the conduct arguably raises concerns under multiple laws.

Read more: <https://www.accc.gov.au/media-release/correction-acc-cc-alleges-google-misled-consumers-about-expanded-use-of-personal-data-0>.

Italian case against Facebook under consumer law

Responsible entity: The Italian Competition Authority (AGCM)

Description: In 2018, the AGCM found Facebook responsible of two unfair commercial practices in breach of the Italian Consumer Code for its privacy and data collection practices (AGCM, 2018^[99]). 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 (Il Tribunale Amministrativo Regionale per il Lazio, 2020^[100]). 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.

Read more:

<https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes>; OECD (2019^[7]).

United States case against Facebook under consumer law

Responsible entity: FTC

Description: 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 (FTC, 2012^[101]). 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 (FTC, 2019^[102]). 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” (FTC, 2019^[103]).

Read more: <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>; OECD (2019^[7]).

Ways to facilitate co-operation between policy areas

Australia’s Digital Platforms Branch

Responsible entity: Australian Competition and Consumer Commission (ACCC)

Description: The ACCC has set up a specialist Digital Platforms Branch to conduct work related to digital platform markets. The Digital Platforms Branch is tasked with scrutinising digital platforms, including undertaking relevant inquiries and current and future consumer and competition law enforcement cases (ACCC, 2020^[104]). The branch was set up after the completion of the ACCC’s Digital Platforms Inquiry in July 2019. The inquiry, undertaken on behalf of the Australian Government, looked at the “impact of digital platforms on consumers and

businesses using platforms to advertise to and reach customers, and news media businesses that also use the platforms to disseminate their content". Following on from this, the ACCC is currently undertaking a range of market inquiries into digital platform services between 2020 and 2025, starting with digital advertising services.

Read More: <https://www.accc.gov.au/focus-areas/digital-platforms>.

Advocacy work in Colombia

Responsible entity: The Superintendence of Industry and Commerce (SIC), Colombia's competition authority

Description: Colombia has experience in using competition advocacy to influence policy making in other spheres. SIC has powers in respect of competition, data protection and consumer protection. The SIC has been involved in competition advocacy that involves: 1) recognising the relevance of compliance with data protection and consumer protection policies, 2) assessing the possible effects on competition of those proposed policies that involve the regulation of data-driven economic activities, and 3) providing recommendations to help mitigate these effects.

- In 2013, the SIC raised possible privacy concerns to the Ministry of Information and Communication Technologies in relation to a draft regulation requiring postal payment service operators to identify customers using personal information such as contact details, occupation, signature and fingerprints.
- In 2017, the SIC considered whether proposals by the Ministry of Transportation regarding the conditions of interoperability of tolls with electronic vehicle payment collection would raise competition concerns. The SIC found that the proposals seemed proportionate and reasonable to enable the different actors in the system to communicate.
- In 2019, the SIC analysed the impact on competition of an administrative act aiming to facilitate cell phone number portability and the economic compensation resulting from failures in calls.
- Also in 2019, the SIC consulted with the Ministry of Trade, Industry and Tourism on the regulation of electronic invoicing, suggesting alternatives that would increase competition by reducing switching costs.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)42/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)42/en/pdf).

Europe's Digital Clearinghouse

Responsible entity: European Data Protection Supervisor (EDPS)

Description: 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 co-ordinate enforcement across Europe's digital sector (EDPS, 2016_[105]). 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, to “help deepen the synergies” and safeguard “the rights and interests of individuals” (European Parliament, 2017^[106]).

The objectives of the Digital Clearinghouse are to: 1) exchange best practices and novel ideas about how to protect individuals in digital markets across legal regimes, and 2) bring together different stakeholders involved in this challenge (Digital Clearinghouse, 2020^[105]). The EDPS hosted four meetings of the Digital Clearinghouse between 2017 and 2018, and from 2019, the Digital Clearinghouse has been jointly hosted by the Research Centre in Information, Law and Society at the University of Namur, the Tilburg Institute for Law, Technology, and Society at Tilburg University, and the European Policy Centre in Brussels. While it is a European initiative, all regulators in the digital space from across the globe are welcome to participate.

Read more: <https://www.digitalclearinghouse.org/>.

Joint study in Italy

Responsible entities: AGCM, the Communications Authority (AGCOM) and the Data Protection Authority

Description: Italy has undertaken a multi-disciplinary approach to data issues by undertaking a joint study on big data involving the competition agency, the communications regulator and data protection agencies (OECD, 2020^[44]). The view was that the complexity of the issues at stake required not only antitrust enforcement, but also adequate advocacy to contribute to an appropriate regulatory framework. Starting from three different policy perspectives, the market study reached the conclusion that the challenges posed by the digital economy cannot be effectively tackled without a common approach, and describes how synergies between the three institutions, equipped with complementary tools, can be effectively achieved whilst respecting each other's issues.

Among its main results, the study showed the low awareness of consumers about the economic value of the data they provide, especially for zero-priced services. That is, where personal data becomes the only value exchanged for the service itself. Moreover, the existence of a “privacy paradox” consisting of a discrepancy between expressed privacy concerns and actual online behaviour can be inferred from the findings of the consumer survey conducted by the AGCM. Almost 93% of the interviewed users were interested in privacy protection, but only one third denied consent to the collection and utilisation of their data.

The three authorities also made important recommendations to policy makers such as measures aimed at reducing information asymmetries at the data collection stage, and facilitating data portability through the development of interoperable systems. Because of this joint initiative, the three authorities have committed to

sign a memorandum of understanding in order to co-operate in a permanent manner in the area of big data.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)33/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)33/en/pdf).

Co-operation in Japan

Responsible entities: JFTC and the Personal Information Protection Committee (PPC)

Description: In Japan, the acquisition, possession or use of personal information by online platforms may be considered an abuse of a superior bargaining position (ASBP) in certain situations under the Anti-monopoly Act (AMA), as discussed above. In addition, there are further protections under Japan's personal data protection law (the PPI Act) (OECD, 2020^[90]). For example, if a company uses or collects personal information without an individual's consent, this is a PPI Act violation. In such cases, the PPC will deal with the case to protect the rights and interests of the individual. However, if the company's conduct is at risk of adversely affecting competition – not just when the individual does not consent, but also when businesses compel consumers to consent to the use of personal information – the JFTC will investigate the case under the AMA. In this way, the JFTC co-operates with the PPC to tackle cases regarding digital platforms and consumers as necessary.

Read more: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)34/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)34/en/pdf).

UK Digital Platforms Taskforce

Responsible entity: Competition and Markets Authority (CMA)

Description: A Digital Platforms Taskforce has been assembled in the United Kingdom (UK Government, 2020^[83]). The taskforce provides a particularly useful example for how cross-policy issues can be addressed. The taskforce is housed within the CMA, headed by a senior CMA official, and comprises staff from the CMA, the Office of Communications (Ofcom), and the Information Commissioner's Office (ICO) (UK Government, 2020^[83]). This is a practical example of how a dedicated group of people with a diverse range of experience can address a wider range of policy issues. In addition, these three agencies have signed Memorandum of Understanding to guide their working arrangements (ICO, 2020^[107]; UK Government, 2014^[108]).

Read more: <https://www.gov.uk/cma-cases/digital-markets-taskforce>.

Multilateral Mutual Assistance and Cooperation Framework for Competition Authorities

Responsible entities: Competition Authorities in Australia, Canada, New Zealand, the United Kingdom and the United States

Description: A Multilateral Mutual Assistance and Cooperation Framework for Competition Authorities has recently been signed between competition agencies in

Australia, Canada, New Zealand, the United Kingdom and the United States (FTC, 2020^[87]). Agreements such as this provide a framework for co-operation between competition agencies across the globe.

Read more: https://www.ftc.gov/system/files/documents/cooperation_agreements/multilateralcompetitionmou.pdf.

References

- ACCC (2020), *Correction: ACCC alleges Google misled consumers about expanded use of personal data*, <https://www.accc.gov.au/media-release/correction-acc-cc-alleges-google-misled-consumers-about-expanded-use-of-personal-data-0> (accessed on 28 July 2020). [98]
- ACCC (2020), *Digital platforms*, <https://www.accc.gov.au/focus-areas/digital-platforms#:~:text=The%20ACCC%20has%20set%20up,and%20competition%20law%20enforcement%20cases.> [104]
- ACCC (2019), *Digital Platforms Inquiry: Final Report*, <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>. [80]
- ACCC (n.d.), *Digital Platforms*, <https://www.accc.gov.au/focus-areas/digital-platforms#:~:text=The%20ACCC%20has%20set%20up,and%20competition%20law%20enforcement%20cases.> [82]
- 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>. [50]
- AGCM (2018), *Facebook – condivisione dati con terzi*. [99]
- 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]
- 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>. [67]
- 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/>. [48]
- Beal, V. (2008), *What are Internet Cookies and What Do They Do?*, https://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp. [16]

- Binns, R. et al. (2018), *Third Party Tracking in the Mobile Ecosystem*, [13]
<http://dx.doi.org/10.1145/3201064.3201089>.
- 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>. [19]
- Bundeskartellamt (2019), *Decision of the Bundeskartellamt B6-22/16 regarding Facebook*, [41]
https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.
- Choi, J., D. Jeon and B. Kim (2019), "Privacy and personal data collection with information externalities", *Journal of Public Economics*, Vol. 173, [53]
<https://doi.org/10.1016/j.jpubeco.2019.02.001>.
- Cisco (2019), *Consumer Privacy Report: The growing imperative of getting of getting data privacy right*, [47]
<https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf>.
- CMA (2016), *Energy Market Investigation*, [45]
<https://assets.publishing.service.gov.uk/media/5773de34e5274a0da3000113/financial-report-energy-market-investigation.pdf>.
- CMA (2016), *Energy Market Investigation*, [66]
<https://assets.publishing.service.gov.uk/media/5773de34e5274a0da3000113/financial-report-energy-market-investigation.pdf>.
- CMA (2015), *The commercial use of consumer data*, [25]
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf.
- 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, [54]
<http://www.kluwerlawonline.com/abstract.php?area=Journals&id=COLA201700>.
- Crémer, J., Y. de Montjoye and H. Schweitzer (2019), *Competition Policy for the Digital Era*, [36]
<https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>.
- Digital Clearinghouse (n.d.), *Digital Clearinghouse*, [107]
<https://www.digitalclearinghouse.org/>.

- 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>. [70]
- 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>. [37]
- 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. [76]
- 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. [105]
- 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]
- Engels, B. (2016), "Data portability among online platforms", *Internet Policy Review*, Vol. 5/2, <http://dx.doi.org/10.14763/2016.2.408>. [69]
- 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 (2016), *Case M.8124 – Microsoft/LinkedIn*, https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf. [62]
- European Commission (2016), *Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions*, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284. [63]
- 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. [79]
- 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. [106]

- 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>. [15]
- 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/JHTLv10i2_Farrell.PDF. [60]
- FTC (2020), *FTC Chairman Joseph J. Simons Signs Antitrust Cooperation Framework with Australia, Canada, New Zealand, and United Kingdom*, https://www.ftc.gov/news-events/press-releases/2020/09/ftc-chairman-simons-signs-antitrust-cooperation-framework?utm_source=govdelivery. [87]
- 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). [103]
- 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. [102]
- 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. [18]
- 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). [101]
- 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. [33]
- 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. [112]

- Gal, M. and D. Rubinfeld (2019), *Data Standardization*, pp. 737-770, [26]
<https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-GalRubinfeld-1.pdf>.
- Gilbert, P. and R. Pepper (2015), *Privacy Considerations in European Merger Control: A Square Peg for a Round Hole*, Competition Policy International, [24]
<https://www.competitionpolicyinternational.com/assets/Uploads/PepperGilbertMay-152.pdf>.
- 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*, [68]
https://www.researchgate.net/publication/281092445_Putting_the_right_to_data_portability_into_a_competition_law_perspective.
- 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, [71]
https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf.
- 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, [57]
<https://www.uclalawreview.org/pdf/61-3-2.pdf>.
- 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, [55]
<http://dx.doi.org/10.2139/ssrn.2533057>.
- IAB (2013), *Cookies on Mobile 101*, <https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf>. [17]
- ICO (2019), *Memorandum of Understanding between the Information Commissioner and Ofcom*, <https://ico.org.uk/media/about-the-ico/documents/2615702/mou-ofcom.pdf>. [86]
- ICO (n.d.), *Working with other bodies*. [109]
- Il Tribunale Amministrativo Regionale per il Lazio (2020), *Altroconsumo, National Consumers' Union and Citizen's Defence Movement v. Facebook*, [100]
https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=tarm&nrg=201815288&nomeFile=202000261_01.html&subDir=Provvedimenti.

- 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>. [38]
- 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>. [35]
- 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. [22]
- 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>. [59]
- 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>. [28]
- 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/. [77]
- 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>. [29]
- Lynskey, O. (2018), *Non-price Effects of Mergers*, OECD Publishing, [https://one.oecd.org/document/DAF/COMP/WD\(2018\)70/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)70/en/pdf). [61]
- 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>. [46]
- 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>. [58]
- OECD (2020), *Consumer data rights and competition*, <https://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm>. [73]

- OECD (2020), *Consumer Data Rights and Competition – Background note by the Secretariat*, [https://one.oecd.org/document/DAF/COMP\(2020\)1/en/pdf](https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf). [5]
- OECD (2020), *Consumer data rights and competition – Note by Brazil*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)41/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)41/en/pdf). [91]
- OECD (2020), *Consumer data rights and competition – Note by Canada*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)31/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)31/en/pdf). [43]
- OECD (2020), *Consumer data rights and competition – Note by Egypt*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)43/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)43/en/pdf). [92]
- OECD (2020), *Consumer data rights and competition – Note by Italy*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)33/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)33/en/pdf). [44]
- OECD (2020), *Consumer data rights and competition – Note by Japan*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)34/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)34/en/pdf). [90]
- OECD (2020), *Consumer data rights and competition – Note by Spain*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)38/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)38/en/pdf). [94]
- OECD (2020), *Consumer data rights and competition – Note by the European Union*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)40/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf). [93]
- OECD (2020), *Consumer data rights and competition – Note by the Russian Federation*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)44/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)44/en/pdf). [95]
- OECD (2020), *Consumer data rights and competition – Note by the United States*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)39/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)39/en/pdf). [97]
- OECD (2020), *Consumer data rights and competition – Note by Turkey*, [https://one.oecd.org/document/DAF/COMP/WD\(2020\)55/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)55/en/pdf). [96]
- OECD (2020), *Digital Advertising Markets*. [40]
- OECD (2020), “Going Digital integrated policy framework”, *OECD Digital Economy Papers*, No. 292, OECD Publishing, Paris, <https://dx.doi.org/10.1787/dc930adc-en>. [72]
- OECD (2019), *Challenges to Consumer Policy in the Digital Age*, <https://www.oecd.org/going-digital/topics/digital-consumers/challenges-to-consumer-policy-in-the-digital-age.pdf>. [75]
- OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264312012-en>. [52]

-
- OECD (2019), "Good practice guide on consumer data", *OECD Digital Economy Papers*, No. 290, OECD Publishing, Paris, <https://dx.doi.org/10.1787/e0040128-en>. [7]
- OECD (2019), "Online advertising: Trends, benefits and risks for consumers", *OECD Digital Economy Papers*, No. 272, OECD Publishing, Paris, <https://dx.doi.org/10.1787/1f42c85d-en>. [20]
- OECD (2018), "Consumer policy and the smart home", *OECD Digital Economy Papers*, No. 268, OECD Publishing, Paris, <https://dx.doi.org/10.1787/e124c34a-en>. [113]
- OECD (2018), "Consumer protection enforcement in a global digital marketplace", *OECD Digital Economy Papers*, No. 266, OECD Publishing, Paris, <https://dx.doi.org/10.1787/f041eead-en>. [88]
- OECD (2018), "Improving online disclosures with behavioural insights", *OECD Digital Economy Papers*, No. 269, OECD Publishing, Paris, <https://dx.doi.org/10.1787/39026ff4-en>. [56]
- OECD (2018), *Non-price effects of mergers*, <https://www.oecd.org/daf/competition/non-price-effects-of-mergers.htm> (accessed on 14 February 2020). [34]
- 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). [32]
- OECD (2018), *Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers*, <https://www.oecd.org/going-digital/topics/digital-consumers/toolkit-for-protecting-digital-consumers.pdf>. [74]
- 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). [31]
- OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>. [8]
- 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), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264229358-en>. [23]

- 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. [4]
- OECD (2007), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352>. [89]
- Ofcom (2016), *Memorandum of understanding between the Competition and Markets Authority and the Office of Communications – concurrent competition powers*, https://www.ofcom.org.uk/_data/assets/pdf_file/0021/83523/cma_and_ofcom_mou_on_use_of_concurrent_consumer_powers_webversion.pdf. [85]
- 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>. [27]
- Podszun, R. (2020), *Facebook @ BGH*, <https://www.d-kart.de/blog/2020/06/23/facebook-bgh/>. [42]
- Purra, J. and N. Carlsson (2016), *Third-Party Tracking on the Web: A Swedish Perspective*, <http://dx.doi.org/10.1109/LCN.2016.14>. [14]
- 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>. [12]
- 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>. [49]
- Rubinfeld, D. and M. Gal (2017), *Access Barriers to Big Data*, p. 339, <https://arizonalawreview.org/pdf/59-2/59arizlrev339.pdf>. [9]
- Ryte (2019), *Tracking Pixel*, https://en.ryte.com/wiki/Tracking_Pixel#What_is_a_tracking_pixel.3F. [21]
- 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>. [65]

- 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. [78]
- Stigler Committee (2019), *Stigler Committee on Digital Platforms, Final Report*,
<https://research.chicagobooth.edu/stigler/media/news/committee-on-digitalplatforms-final-report>. [81]
- Stucke, M. (2018), *Should We Be Concerned About Data-opolies?*, p. 275,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144045. [39]
- 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. [111]
- Turow, J. (2017), *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*, Yale University Press. [10]
- UK Government (2020), *Digital markets taskforce: terms of reference*,
<https://www.gov.uk/government/publications/digital-markets-taskforce-terms-of-reference/digital-markets-taskforce-terms-of-reference--3>. [83]
- UK Government (2015), *CMA and ICO memorandum of understanding*,
<https://www.gov.uk/government/publications/cma-and-ico-memorandum-of-understanding>. [84]
- UK Government (2014), *CMA and Ofcom memorandum of understanding*,
<https://www.gov.uk/government/publications/cma-and-ofcom-memorandum-of-understanding>. [110]
- 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>. [64]
- 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. [51]
- Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs. [11]