Organisation for Economic Co-operation and Development

DAF/COMP/WD(2020)59

Unclassified English - Or. English

31 July 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Cancels & replaces the same document of 5 June 2020

Consumer data rights and competition – Summaries of contributions

12 June 2020

This document reproduces summaries of contributions submitted for Item 3 of the 133rd Competition Committee meeting on 10-16 June 2020.

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

Please contact Ms Anna BARKER if you have questions about this document.
[Email: Anna.BARKER@oecd.org]

JT03464375

Table of Contents

Summaries of contributions 3
BEUC 4
BIAC 6
Brazil 7
Canada 8
Colombia 9
Egypt 10
EU 11
Germany 12
Italy 13
Japan 14
Mexico (IFT) 15
Portugal 16
Russian Federation 18
Spain 19
TUAC 20
Turkey 21
Ukraine 22
United Kingdom 23
United States 25

Summaries of contributions

This document contains summaries of the various written contributions received for the discussion on consumer data rights and competition (133rd Meeting of the Competition Committee on 10-16 June 2020). When the authors did not submit their own summary, the OECD Competition Division Secretariat summarised the contribution. Summaries by the OECD Secretariat are indicated by an *.

BEUC

In the EU, the General Data Protection Regulation (GDPR) contains some pro-competition provisions like the portability right (Article 20), but it falls short in providing effective means to help consumers to port their data to competing service providers. In this regard, Article 20 of the GDPR provides for a general right to data portability as regards personal data, which is not just a right to strengthen the data subject's autonomy, but has been conceived as a tool to *'support the free flow of personal data in the EU and foster competition between controllers'*. However, this right has several limitations. First, portability only applies to personal data and therefore excludes other data that could be useful to allow portability between services. Secondly, it applies to data 'provided' by the data subject, excluding data inferred and derived by the data controller. From a competition perspective, the portability right of the GDPR does not entail specific interoperability obligations enabling new entrants to interact with the data holder's service. That is why BEUC welcomes that the Commission plans in the context of its Data Strategy of February 2020 to adopt measures to enhance the portability right under Article 20 of the GDPR in its upcoming Data Act.

Progress has been made however in sectoral legislation. Mandatory data access, interoperability and access to application programming interfaces exists in sector-specific EU laws in the field of financial services, after-sales services for vehicles and energy grid data: namely the Payment Services Directive (PSD2), the Type Approval Regulation and the revised Electricity Directive. These instruments impose obligations on the data holders or incumbents to enable access to data, for example in the case of open banking, through an application programming interface (API), so that other operators are able to provide services to consumers. Although the nature of the data concerned is different, due to the particularities of the markets concerned, the obligations under these instruments all seek to address market failures. These pro-competition measures are designed in the light of that objective, something that it is not necessarily the case with other EU laws, which aim to protect other issues (e.g. data protection or intellectual property). But these examples of pro-competition legislation often fail to deal specifically with the role of consumers in such access regimes, in particular concerning consumer permission to access his or her personal data.

Therefore, BEUC recommends that decision-makers (e.g. when regulating data access regimes) and enforcement authorities (e.g. when designing data access remedies) take into account the following principles for a consumer-friendly data-driven and competitive ecosystem:

- Intervention in the form of data access should be used only to tackle market failures leading to higher consumer prices, less choice and less innovation.
- Data access must foster the development of consumer-centric innovation.
- Consumers must be allowed to object to sharing of their personal data when the sharing has been mandated by law. This right does not exist under the General Data Protection Regulation (GDPR) and therefore should be further considered by the legislator as an additional requirement when adopting data access regimes or as a condition for the data sharing if mandated by a competition authority as an interim measure or competition remedy.

- Operators handling personal data must be obliged to establish a high-level of data security.
- Consumers must be offered technical solutions to help them to control and manage flows of their personal information.
- Consumers must have access to redress when these principles are not respected

BIAC

The level of collection of consumer data, as well as its value, is unprecedented and growing daily. The collection and use of consumer data can be a powerful driver of business efficiency and innovation, which can create significant benefits for consumers. For example, as a result of having their data collected, consumers can receive personalized offers for products and services likely to be of most relevance, interest and usefulness to them.

At the same time, the collection and use of consumers' data may raise novel issues around protection, including those related to consumer protection and competition. Users of digital products, including apps, social media platforms and websites, may worry about how their data is being used and discussion often focuses on the apparent trade off that users are asked to make between privacy and the usefulness and cost of digital services.

It is important to note, at the outset, that, while consumer protection and competition laws are aimed at ensuring better outcomes for consumers, whether that is in the form of lower prices and higher quality resulting from a vibrant competitive process, or of avoided individual harms from unfair or exploitative practices, the regimes also pursue goals that can pull in different directions. For example, to the extent that competition law identifies data to be an important input, the wider availability of which would stimulate competition, privacy laws can rightly restrict the sharing of data that is personal. Given how rapidly technology is evolving, certainty and predictability of enforcement are vital to realizing the benefits of technology, while simultaneously addressing true market failures in a manner that does not unnecessarily chill innovation and investment. These comments focus on the positive and normative role of competition law enforcement as it encounters the challenges associated with consumer data rights.

While a lack of consensus exists about the ethics and preferences surrounding consumer data collection, it is indisputable that consumer data has become an important, and valuable aspect of e-commerce, digital platform businesses, and societal progress. *Business at OECD* supports minimizing the negative consequences associated with data-based developments without compromising their positive outcomes. Delineating the ideal scope of competition law alongside the evolving sphere of consumer data rights, including privacy, is essential to ensuring that regulators and policymakers work within their perimeters and avoid overregulation, which would create issues as opposed to resolve them.

Business at OECD therefore recommends that continued responsibility for enforcing market failures relating to consumer protection remain with consumer protection agencies, including those governing privacy, and that these agencies and competition authorities coordinate their advocacy and enforcement activities, where needed. Regulatory overlap should be avoided (or at least minimized) to increase certainty and predictability for consumers and businesses alike. Where evidence substantiates that business' collection or use of consumer data causes harm to competition such as by erecting barriers to entry or through an absence of non-price competition, then any such market failure may be addressed under existing tools of competition enforcement.

Brazil

Consumer data rights include a broad array of rights other than just privacy, such as the right to portability, which is aimed at empowering consumers, giving them more control over their own data. Regarding competition, possible outcomes of this increased control could be higher output, better quality, lower prices, and, especially, with the emergence of competitors that can effectively constraint incumbents' decisions, lower costs for switching providers.

On this matter, the Administrative Council for Economic Defense (CADE in Portuguese) has an ongoing investigation into the financial sector. On one hand, this sector has been for a long time a heavy user of personal and transactional data. On the other hand, it is highly concentrated in Brazil, as it is in various countries. In this sense, the impacts of avoiding data sharing must be assessed, including when the alleged reason is protecting consumers' privacy.

The various aspects that arose throughout this investigation[1] provide a useful framework for the discussion on the impacts on competition related to consumer data rights. Some particularities include the non-rival aspect of data, which differs from other inputs, especially tangible ones; the possible entry barriers linked to the control and availability of consumers' data in an information-intensive sector; and the assessment of the dynamic effects (especially on businesses' incentives to invest and innovate) of a possible imposition to force institutions to provide access to data.

1 The views expressed in this document do not necessarily represent CADE's opinion regarding the case at issue and are merely brought as a contribution to the discussion on consumer data rights and its impact on competition.

Canada

The rapid rise of the digital economy is a borderless phenomenon that requires close collaboration and cooperation between competition authorities. In its submission, the Competition Bureau of Canada ("Bureau") describes its past enforcement and advocacy efforts relevant to businesses' collection and use of consumer data. Through its enforcement experiences, the Bureau has identified situations where businesses have used data to exercise market power, erect barriers to entry, and engage in deceptive marketing practices. In the advocacy context, the Bureau has recognized opportunities for governments to enact pro-competitive policies supported by data portability and open data standards. Given its importance as a key driver in the modern economy, the Bureau will continue to place a strong focus on digital economy matters going forward.

Colombia

This submission discusses the state of play of the protection of data rights of consumers under the Colombian Data Protection, Consumer Protection and Competition Protection Regimes. To that effect we will present the way those rights are interpreted and enforced under our applicable regulations. We will provide a short description of the concepts that are key to the present discussion from our jurisdictions perspective and finally we will address, through some case examples, the roles of both Consumer Protection and Competition Protection enforcement and advocacy actions towards the protection of those rights.

The Superintendence of Industry and Commerce (SIC) has enforced and advised on the protection of data rights of consumers. Through decisions from its Deputy Superintendences and involvement in international venues, the SIC has recognised the importance of guaranteeing consumers access to and control of their data. Also, the SIC has examined, among others, the potential effects of the abuse of targeted advertisement over consumers decision-making; unfair contract clauses in e-commerce transactions to collect large amounts of data; unfair and deceptive practices in connection with the collection, use and disclosure of personal data to third parties and the competition impacts of data portability.

Egypt

The commodification of consumer's personal data has led the Egyptian Competition Authority (ECA) to intervene in the domain of data rights protection in order to carry out its role. ECA's role has two main aspects, which are the protection of the freedom of competition and consumer's welfare, and the exploitation of consumer's data rights which could harm these objectives.

Data collected by firms, notably in the digital markets, is an asset that it can be sold to third parties in order to make profit on the other side of a "zero-price" service, i.e. social networks and search engines. However, in markets where data is integral to the activity of the firm, data becomes the "oil" that fuels the economic activity on this market meaning that it becomes a source of market power allowing firms to predict the behavior of consumers and competitors and acting independently of them. In data-heavy services, the existence of a player that owns a significant amount of data in a market entrenches his dominant position and creates significant barriers to entry.

This is especially true in an economy similar to Egypt's, where data and databases are scarce, the collection of data is costly in time and there is a lack of financial resources. Firms that possess this data, possess an unfair competitive advantage as data is ultimately owned by consumers. Nevertheless, consumers are not aware of the types of data that are being collected or how it is being used. Firms analyse the collected data in order to train their algorithms and draw out conclusions on consumer and market behavior.

The conclusions that firms draw from this data allows them to exploit consumers. The algorithms predict what consumers are willing to accept in terms of price and quality. "The willingness to pay" indicates the highest price each consumer is willing to pay and hence allows firms to personalise the prices they provide to consumers, which may result in exploitative price discrimination. In addition, firms take advantage of the "privacy paradox", and the fact that consumers underestimate the value of the personal data they give in exchange of a "zero-price" service.

ECA occasionally implements remedies in the framework of mergers in order to restore consumer's data rights to privacy and portability and use data as an incentive to new entry in the market. This was evident in the case of Uber's acquisition of Careem, its biggest competitor in the Middle East and North Africa (MENA) region, where ECA imposed data portability and data sharing remedies on the parties. ECA believes that allowing data access to potential entrants will restore the competition to pre-transaction levels and may create a new area of competition on offering the highest standard of privacy.

ECA believes in the role of competition authorities to cooperate with data protection authorities in order to protect consumer data rights and ultimately consumer welfare. However, ECA believes that the optimal method to limit violation of privacy rights is to increase digital awareness and to foster competition on the market where every market player competes to offer better privacy standards to consumers.

EU

The collection and use of consumer data by businesses and other entities, together with the harms associated with violations of privacy, have garnered increasing attention from the public and from civil society in recent years. In this context, privacy and data protection legislation has gained in visibility and importance, in parallel with increasing attention focused on the phenomenon of big data and the 'gatekeeper' role played by large digital platforms occupying pivotal points in the online environment.

In the EU, the General Data Protection Regulation (GDPR)[2] became applicable in May 2018, replacing and modernising the previous Data Protection Directive (Directive 95/46/EC) and harmonising the data protection laws of the Member States, as well as introducing a new enforcement system with the possibility of imposing fines on undertakings and other entities. The GDPR has strengthened the control held by individuals over their data, including by reinforcing certain rights held by individuals (known as 'data subjects') already under the previous regime. It notably has also introduced a new general right to data portability of a data subject's personal data from one economic operator to another (Article 20).

In this context, a debate has arisen in the EU and globally around the interaction between, on the one hand, data protection laws and the rights bestowed on consumers in relation to their fundamental right to privacy and personal data and, on the other hand, competition policy and enforcement. This contribution outlines the European Commission's initiatives and experience in this area and summarises a few legal and policy questions that merit further consideration in the years ahead.

Part 1 outlines the collection and use of consumer data in today's marketplace, in particular in relation to undertakings that rely on the processing of personal data[3] for the majority of their revenue via the provision of advertising services. Further, consumer attitudes towards consumer data collection and use are considered in light of opinion surveys and academic literature.

Part 2 describes the EU's regulatory framework for consumer data rights, with particular focus on the GDPR, including the right to data portability. This part concludes with a forward-looking outline of potential initiatives to strengthen consumer data rights in the context of the European Commission's strategy for data.

Part 3 describes potential theories of harm involving consumer data-driven markets and discusses the available case precedents. Both merger control and antitrust enforcement are covered. Then, this part concludes the paper by briefly addressing (selected) analytical challenges identified, that complicate competition assessments in cases relating to the collection and use of consumer data. The discussion of the challenges is not meant to (and cannot) be exhaustive, but only to highlight a few new directions in which further work is likely to be needed in the future.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR").

[3] Article 4(1) GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Germany

Collecting, storing, analysing and monetising data plays an important role in modern, data-driven economies. Consequently, access to data plays a key role in the digital economy and personal data is of particular interest. The dynamics in data collection have changed the dynamics in many markets and raised difficult competition law issues at the intersection between competition, consumer protection and privacy that need to be considered. The core mission of competition authorities is to keep markets open and ensure fair competition, which will also benefit consumers.

Italy

Addressing the impacts on competition of consumer data rights offers a valuable opportunity for the Italian Competition Authority (the Authority or the ICA) to present its competition enforcement and consumer protection experience, as well as the findings of the big data market study (the Study), conducted jointly with the Communications Authority (AGCOM) and the Data Protection Authority.

The complexity of the issues that emerge when consumer data rights are a relevant consideration requires not only antitrust enforcement, but also adequate advocacy in order to contribute to the definition of an appropriate regulatory framework.

In its competition enforcement activity, the ICA has ascertained exclusionary abuses of dominant position in the energy sector based on traditional leverage theories of harm also when consumer data rights play a key role. Recently, the ICA has opened a case for an alleged refusal to deal by a dominant player in the digital space.

Recognizing that in the digital economy competition may overlap with other public policy objectives, especially in relation to consumer data rights, the ICA, the AGCOM and the Data Protection Authority decided to privilege a multi-disciplinary approach undertaking a joint initiative. Starting from three different perspectives, the Study reaches 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 missions. In relation to consumer data rights, the three authorities have made important recommendations to policymakers, such as measures aimed at reducing information asymmetry at the data collection stage and facilitating data portability also through the development of interoperable standards.

Consumer protection may play a relevant role in dealing with some of the issues that emerge when dealing with consumer data right, especially in reducing information asymmetry between users and digital operators in order to allow consumers to exercise their choices knowingly and effectively. Agencies tasked with a dual competence in the antitrust and consumer protection fields may be facilitated in dealing with consumer data rights, as coordination costs of the two policies can be in principle substantially lower and the assessment of the issues at the intersection can occur even at the case level.

Lastly, the Covid-19 pandemic may add the protection of public health as another public policy objective to the access to and utilisation of consumer data rights. Responses to the current crisis might exacerbate some of the trade-offs that have so far been acknowledged, in particular between competition and privacy.

Japan

Facing concerns raised by various stakeholders and experts regarding competitive impact of acquiring and accumulating vast amount of personal data by platforms, the Japan Fair Trade Commission (JFTC) held the study group and published fundamental principles (2018) which proposed that it was necessary to discuss how the regulation of abuse of superior bargaining position (ASBP) could be applied to the conduct of business platforms against consumers providing the platforms with their own personal data under the Antimonopoly Act (AMA), together with the other ministries related to economic policy and telecommunication.

Against the background, the JFTC published the new Guidelines (2019), by clarifying what kind of conducts to acquire, possess or use personal information, etc. could be regarded as ASBP under the AMA.

Although the regulation of the "Act on the Protection of Personal Information" (PPI Act) is different from the one of ASBP in terms of not just intent and purpose of the regulations but also their coverage, the JFTC, as necessary, cooperates with the Personal Information Protection Committee operating the PPI Act to tackle the cases.

Mexico (IFT)

In Mexico, consumer data rights are established in the Federal Law on the Protection of Personal Data in Possession of Private Parties and the General Law for Protection of Personal Data in Possession of Obligated Subjects, enforced by the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI), and in the Federal Telecommunications and Broadcasting Law (LFTR), enforced by the Federal Telecommunications Institute (IFT in Spanish), as the exclusive competition authority for the telecommunications sector, which has the mandate of guaranteeing competition and free market access. This contribution focuses on the latter.

In the telecommunications sector, there is a large amount of information that can be valuable for companies. The LFTR recognises a series of rights for the user of telecommunications services including, among others, the protection of their personal data (name, address, email, telephone number, geographic location, type of mobile communications equipment, among others) and free number portability.

Service providers have the obligation to inform the user, through a privacy notice, which data they will collect and for what purposes. Users have the right to authorise that their data is used only for the purposes they approve and, at all times, they have the right to the security of safeguarding them. Users can Access, Rectify, Cancel their information and Oppose to its use (ARCO rights). Also, the user has the right to have its provider safeguard and protect its communications, as well as the data that identifies it (date, time and duration of calls, messages or data that identify the origin and destination of these, among others), guaranteeing its confidentiality and privacy.

Likewise, number portability facilitates the user's decision regarding the choice of its service provider, which has contributed to a substantial improvement in the quality of services, a greater offer of products and a reduction in rates, due to the fact that competition has been strengthened and service providers have had to strive to retain and attract users.

The LFTR also establishes data conservation obligations for the service providers. They have to keep records and controls of any communication made from any type of line with owned or leased numbering, in any form, to identify information accurately and necessary to collaborate with the competent authorities, in matters of security and justice, against criminal conduct. Furthermore, the LFTR establishes specific *ex ante* measures for the preponderant economic agent (incumbent) in order to reduce information asymmetries, which have been identified by specialised courts as market failures; to establish a level playing field; and to promote competition.

Portugal

The collection and use of data have become widespread among digital firms. The AdC has followed these developments closely and taken an interest on how they may impact the way in which competition plays out in (digital) markets. The AdC has published an Issues Paper in 2018 on the FinTech and InsurTech sector in Portugal, addressing barriers to entry and expansion related to data access.[4] In 2019, the AdC published an Issues Paper on the digital economy,[5] highlighting how data can be a source of competitive advantage for digital firms and, hence, how lack of access to data, both in a timely fashion and in a sufficient extent, may pose significant barriers to entry and expansion.

Digital firms may use the data they collect about their users to increase the quality of the services they provide. The nature of data as an input in digital services and the possibility of data-driven network effects imply that lack of access to data may raise significant barriers to entry and expansion in digital markets.

Consumer data rights can mitigate barriers to entry and expansion in digital markets related to data by effectively giving ownership of data to consumers and allow them a greater control over how their data is used. In particular, consumer data rights legislation may establish a right of data portability, such as article 20 of the GDPR in the EU.

Data portability legislation, nonetheless, may have several limitations that hamper its ability to reduce barriers to entry and to expansion due to the lack of access to data.

Firms may have an incentive to impose costs or to exploit consumer behavioural biases to limit the number of data transfers or the volume of data transferred to other platforms. This may be done by strategically imposing to users unnecessary additional hurdles to download or to transfer their data, such as additional buttons or windows to click through, unfriendly user interfaces, or additional authentication steps. The exploitation of consumer behavioural biases can be curtailed by reducing the degrees of freedom digital platforms have in how they design the proceedings for data transfer requests, the user interfaces or consent forms.

Data portability may not be enough if data is very heterogeneous or there are significant costs or barriers to algorithm development. It may also be the case that one can only extract valuable insights from data subject to data portability, if it is analysed in conjunction with other data not subject to data portability.

There may be a complex interplay between privacy and competition that may make the effect of additional data collection on consumer welfare more complex. Consumers can prefer to use platforms that collect less data about them, all else the same.

Consumer behavioural biases may also be exploited so that firms can collect more data about their users.

[4] Available at: http://www.concorrencia.pt/vEN/Estudos_e_Publicacoes/Estudos_Economicos/Banca_e_Seguros/Pages/Executive-Summary-Issues-Paper.aspx?lst=1

[5] Available at: http://www.concorrencia.pt/vPT/Estudos_e_Publicacoes/Estudos_Economicos/Outros/Documents/Digital%20Ecosystems,%20Big%20Data%20and%20Algorithms%20-%20Issues%20Paper.pdf

The degree of consumer privacy may also shape how competition plays in the market, namely by allowing firms to focus on more captive consumers, on less informed consumers or on consumers more subject to behavioural biases. Bias exploitation can be employed to reduce competition or induce users into making unwanted purchases, as firms learn how to better divert consumers to certain products. Firms may also data to adopt market segmentation strategies, and potentially limit the extent of competition in the market and extract more surplus.

Russian Federation

Data of consumers of digital services is not only an important resource for developing the economy and personalising offers on the market, but also an integral characteristic of the individual user and his autonomy.

Despite the fact that the data itself is non-rivalrous and in general it is not difficult to obtain it, and companies can quickly collect large amounts of data, some categories of data – primarily personal user data – need special processing and use protection measures.

The control over the processing and use of user data is realised by competent regulators. It should not be allowed that the data received by market participants is used unfairly as a competitive advantage and exclusive access to such data hinders the development of competition in the market.

The Federal Antimonopoly Service of Russia (FAS Russia) is fully aware of the need to control the non-rivalrous use of data in digital markets, while in the process of considering cases involving the consumer data rights, and guided by Federal Law of 27 July, 2006 No. 152-FZ "On Personal Data" in conjunction with Federal Law of 26 July 2006 No. 135-FZ "On Protection of Competition".

In order to develop data of the FAS Russia, Federal Law "On Amending the Federal Law "On Protection of Competition" and other legislative acts of the Russian Federation" (the fifth antimonopoly package) has been drafted, which includes changes to antimonopoly legislation in the context of digital economy.

Work of the FAS Russia on modernisation of legislation and enforcement in the context of digital economy is part of the work of competition authorities and international organisations around the world to address changes that emergence of digital markets entails for the economy and consumers. The FAS Russia is ready to continue, as well as in cooperation with foreign partners, to monitor dynamics of digital markets development and participate in the generation of best practices for their regulation.

Spain

The ability to collect, refine and exploit (consumers') data is becoming a key source of competitive advantage in the digital economy. Firms tend to manage data in-house and rarely sell them, since data is a key asset due to factors as scale, learning, scope and network effects. This may create barriers to entry and growth for new and small competitors and dynamics of market concentration. Another market failure could be the asymmetric information faced by consumers in terms of awareness of the use of their data.

Regarding competition law enforcement, especially in recent years, the National Commission for Markets and Competition (CNMC in Spanish) has assessed a number of cases in which issues related with data have played a relevant role. Moreover, in mergers that have impact in digital markets the CNMC typically evaluates the rationality of the operation in order to detect whether one of the objectives of the merger is to acquire access to customer information which can give rise to concern in the sense that it could place the acquirer's competitors at an unjustified disadvantage and raise barriers for market entry.

As for competition advocacy, the CNMC has actively analysed data issues in several markets disrupted by digitization. Data portability has been praised as a procompetitive principle in CNMC's work on the sharing economy. Open banking principles, such as technological neutrality and interoperability, were commended in the CNMC's market study on Fintech. Currently, the CNMC is carrying out a market study on online advertising and is following the national, European and multilateral debates on data issues and digital markets.

TUAC

On the occasion of a roundtable on "consumer data rights and competition", the OECD Competition Committee will discuss the ways in which businesses collect and use consumer data and the role of competition enforcement. In a background note, the OECD describes the increasing use of consumer data in a digitalised economy.[6] Potential harm to competition may arise where firms are unwilling (data capture) or unable to share their data (insufficient interoperability may hinder market entries). Furthermore, the substantial economic value of consumer data has to be balanced with the risks to consumer's privacy.

Overall, TUAC agrees that achieving interoperability of platforms, processing and sharing systems is important to achieve markets that are more competitive. This is also in the interest of job creation and the ability of individuals to handle data across sectors and applications. The trade union movement is indeed very concerned about the market power of highly digitalised businesses.

This contribution seeks to bring the attention of competition authorities to the workplace dimension of data and to call for appropriate competition enforcement.

The risks associated with consumer and personal data are an important topic and an array of protective regulations is being put in place at national and regional level (e.g. GDPR). In contrast, the abusive collection and use of workers' data is gathering less recognition. Yet, their impact on individual liberties (including the privacy of workers) and unbalanced labour relations is undeniable.

[6] OECD (2020), *Consumer Data Rights and Competition - Background note by the Secretariat*, http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm

Turkey

In recent years, together with the rise of digital economy and big data-driven industries, concerns related to privacy has increased enormously, which caused an important concern to rise: How privacy should be considered within the context of competition law? Do these two areas of law intersect? Is it possible to handle privacy as a matter of quality of the service offered by a platform? Can the competition authorities build theories of harm based on privacy concerns?

Regarding the area of competition law, Turkish Competition Authority (hereinafter the "TCA") has been keeping a close eye on digital sector, especially on online platforms which are in dominant position, mostly through broad investigations starting nearly from 2015 to 2020. Moreover, TCA announced in late January 2020 that it has initiated a sector inquiry named "The Report on Digitalisation and Competition Policy" to determine the competition policies in digital sectors by closely following the national and international developments in this field.[7] In addition to that, TCA has recently empowered its already existing Strategy Development Department to catch up with the new developments in digital markets.[8]

On the other hand, regarding the area of data protection law, Turkish Data Protection Law No. 6698 (hereinafter the "Data Protection Law") has come into force on April 7th 2016, which is prepared based on Directive 95/46/EC on data protection (Data Protection Directive). Although the rights of the data subjects in the Data Protection Law and GDPR are similar to a large extent, the differences cannot be undermined. For example, the Data Protection Law does not involve the right of access by the data subject, right to be forgotten, right to restriction of processing and right to data portability to other consented data controller.

So far, there seems to be no intersection between the area of competition law and data protection law in Turkey since the two are still handled as parallel issues. Although there have been cases[9] referring to the importance of data as a competition parameter, there have been no competition law cases dealing with privacy related concerns so far. This is partially because the landmark mergers in which privacy-related concerns were most likely to be discussed such as WhatsApp's acquisition by Facebook were below the revenue thresholds of TCA. In addition to that, Data Protection Law does not involve the right to data portability, which might be a potential factor increasing the responsibility of TCA in eliminating the entry barriers for competitors and increasing the consumer welfare. Therefore TCA seems to have a greater role than other competition authorities within the EU in compensating the shortcomings of the Data Protection Law, which lacks the right to data portability.

7 TCA's Press Release dated 30.01.2020. Available only in Turkish at: https://www.rekabet.gov.tr/tr/Guncel/rekabet-kurumu-dijitallesme-ve-rekabet-p-874d77d25943ea118119005056b1ce21 .

8 TCA's press release dated 08.05.2020. Available only in Turkish at: https://www.rekabet.gov.tr/tr/Guncel/rekabet-kurulu-dijital-ekonomiyi-mercek--61aedbe40a91ea11811a00505694b4c6 .

9 TCA's AEH/Migros decision dated 09.07.2015 and numbered 15-29/420-117. Available only in Turkish at: https://www.rekabet.gov.tr/Karar?kararId=57e9efbd-fda1-4f78-b985-6a1542c88cd2 ; TCA's CK decision dated 20.02.2018 and numbered 18-06/101-52. Available only in Turkish at: https://www.rekabet.gov.tr/Karar?kararId=537b366a-8bd7-4821-8760-43592452b711; TCA's EnerjiSa decision dated 08.08.2018 and numbered 18-27/461-224. Avalable only in Turkish at: https://www.rekabet.gov.tr/Karar?kararId=b6989e2e-27ce-4ded-8591-05b0b23c86c1 .

Ukraine

The Law of Ukraine "On Personal Data Protection" regulates legal relations concerning protection and processing of personal data. It is aimed at the protection of fundamental rights and freedoms of a person and citizen, in particular, the right to non-interference with privacy in connection with the processing of personal data operates in Ukraine. According to it, personal data is information, or a set of information about an individual that is identified or can be accurately defined (i.e., individualised consumer data).

Ukrainian legislation also establishes mechanism for the protection of confidential information about economic entities and their customers, which are used by the Antimonopoly Committee of Ukraine (AMCU). AMCU and its employees are responsible for not disclosing of commercial secret defined by the Law.

Another Law – "On Protection against Unfair Competition" – protects the access to consumer information, acquires commercial secret status and the restriction of access to it.

On the other hand, availability of individualised consumer information is a necessary element for the certain economic activities, which in particular involves the establishment and periodic renewal of direct contractual relations between the supplier and the customer. The importance of customer data as a source of market power strengthening is critical on market with a limited number of consumers, and contracts with them have a long-term character. In such circumstances, the limited access to consumer data may serve as a barrier to entry.

Recently AMCU intervened in anticompetitive practices related to customer data access.

It's worth to mention the AMCU's decision from Dec 2018. The information on the full list of suppliers and customers with contact details and concluded contracts were took away by co-founder of the company and used to "steal" customers to newly founded business. It happened despite the fact that above-mentioned former co-owner of the first company signed obligations to maintain commercial secrets for three years after dismissal, in particular, undertook a duty not to use information that may harm the original company. The AMCU recognised the violation of Article 19 of the Law of Ukraine "On protection against unfair competition" in this case.

United Kingdom

Use of consumer data and market failures

The Competition and Markets Authority (CMA) acknowledges the clear benefits to consumers, businesses and the economy from the use of consumer data, as described in the background paper. The CMA also, however, recognises the risks of market failures arising from the collection and use of consumer data. The CMA has been considering these issues across a range of its work for a number of years, most recently in its review of merger control, its Digital Strategy and in its ongoing Online Platforms and Digital Advertising Market Study.

In summary, market failures relating to consumer data may arise on the supply or demand side. Market failures may particularly arise in digital platform markets which tend towards high concentration as a result of a number of features, including preferential access to data. On the supply side, this may occur where new entrants are unable to enter the market because data-related barriers to entry or expansion are too high. On the demand side, this may occur in particular when consumers have insufficient knowledge and control over how data are collected and used.

In broad terms, we have identified the following potential failures and corresponding measures necessary to address them:

- **Data access measures:** Measures to open up competition by enabling challengers to access consumer data held by an incumbent which is needed to promote new services. These measures may engage data protection or privacy considerations insofar as the data being accessed is 'personal data' under data protection law.
- **Data mobility measures**: Measures to promote new entry by enabling new providers to create innovative ancillary services which interoperate with existing systems. Insofar as personal data created or processed on one system is used for another, this may raise data protection issues of consent and repurposing.
- **Measures to enhance consumer choice:** Measures to enable consumers to exercise greater choice over data collection and use to discipline businesses over data collection practices. These include measures to ensure that defaults do not unduly favour particular participants; measures to ensure that choice mechanisms consistently respect consumer choice over time; and measures to impose a 'fairness by design' duty to promote consumer choice.

What is the role for competition enforcement?

The background paper identifies two ways in which privacy assessments may be relevant to competition assessments; (i) as an aspect of quality on which businesses may compete, and (ii) that the collection and ownership of consumer data, and access to that information, may have competition implications.

On the first question, the CMA considers that, in some respects, data protection and privacy rights can be seen as an aspect of quality over which businesses compete, and this is reflected in merger control decisions. However, privacy and data protection rights cannot be reduced simply to aspects of quality because they engage fundamental rights which are at the heart of citizenship. Competition authorities are not well placed to address these issues: competition and non-competition concerns should be assessed separately by different decision-makers.

On the second issue, the CMA strongly agrees that the collection and use of consumer data can have significant competition impacts, in particular that, in combination with other features

which may characterise the digital platform economy, it may contribute to a form of enduring market power which can be exploited. This is an issue being explored in our Online Platforms and Digital Advertising Market Study.

The CMA agrees that competition enforcement could be used in appropriate cases when it is possible to demonstrate abuse of dominance (or anti-competitive agreements). However, enforcement is an ex post measure which is backward looking and slow. The CMA has broadly accepted the case made in the report of the Digital Competition Expert Panel (DCEP) that there is likely to be a need for ex ante regulation to complement ex post regulation.

The DCEP report proposed a code of conduct which would apply to digital platforms that have been designated as having a 'strategic market status'. The CMA is currently examining these issues and proposed interventions in its Online Platforms and Digital Advertising Market Study and in the Digital Taskforce. In the context of this paper, a code of conduct may include enhanced measures to promote consumer choice, for example through an obligation to trial and test the effectiveness of choice mechanisms.

What is the role for competition advocacy?

We strongly agree that there is a role for competition policy to promote better consumer outcomes for markets involving consumer data, and that this should actively be pursued in cooperation with consumer and data protection agencies nationally and internationally.

Competition and data protection policy have similar broad objectives of promoting the welfare of individuals for the benefit of society. For the most part these two objectives are aligned (for example control over data, as outlined above). However, on occasion, measures to promote individual privacy protections may potentially reduce the level of competition in a market and vice versa.

In these cases, it is important that the respective authorities can engage in a dialogue based on the common goal of maximising consumer welfare. For example, in the CMA's Online Platforms and Digital Advertising Market Study, the CMA advocated joint consideration of the risk that aspects of the design and interpretation of current data protection regulation favour the business model of large, vertically-integrated platforms over smaller, non-vertically-integrated publishers. We are continuing to engage with the Information Commissioner's Office (ICO), the UK data protection authority, in relation to this issue.

The remedies outlined above all potentially involve, to a greater or lesser degree, a potential interaction with data protection and privacy rights. Competition and data protection authorities should work together to explore these issues and future developments and technologies which might promote more competitive markets while maintaining privacy protections.

United States