Organisation for Economic Co-operation and Development

DAF/COMP/M(2020)1/ANN5/FINAL

Unclassified

English - Or. English

29 October 2021

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Summary of discussion of the roundtable on Consumer data rights and competition

Annex to the Summary Record of the 133rd Meeting of the Competition Committee, held virtually on 10-16 June 2020

12 June 2020

This document is the summary of discussion of the Roundtable on Consumer Data Rights and Competition held during the 133rd meeting of the Competion Committee.

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

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

JT03484089

Summary of discussion of the roundtable on Consumer Data Rights and Competition

This paper, prepared by the Secretariat, provides a summary of the discussion that took place as part of a Competition Committee Roundtable on Consumer Data Rights and Competition, which took place virtually on 12 June 2020.

Introductory remarks

The **Chairman** welcomed participants and introduced the topic of the roundtable: consumer data rights and impacts on competition. He noted that a number of countries across the globe have recently enacted a range of new consumer data rights. Further, there is increasing discussion about the interplay between competition, consumer protection, and privacy and data protection policies and law. In particular, the way that consumer data rights are developed and implemented can potentially affect competition in certain markets. For example, by raising barriers to entry or changing incentives. Further, certain desirable competition remedies may have the effect of lessening the level of protection of consumer data. This means that some co-operation between competition and data protection agencies is required.

The Chairman noted that there are also questions about how far competition authorities should go in considering existing consumer data rights and issues of privacy and data protection when they assess competition issues. In this respect, and regarding the historical development of these issues, the Chairman quoted Zanfir-Fortuna and Ianc (2019[1]):

> *At the beginning, competition authorities were acknowledging data protection law as being a separate issue without relevance for the purpose of merger control proceedings and thus placing the two areas of law on parallel pathways. In a second phase, the realization that data protection rules may in fact have a role in hampering or enabling competition took more and more space both in policymaking and in adjudication, with Data Protection Authorities starting to play a role.*
>
> *We are currently at the dawn of [a] third phase … [where] data protection law considerations are at the core …*

The Chairman noted that Zanfir-Fortuna and Ianc (2019[1]) call this third phase the "Uberprotection phase", defined as the protection of the rights of individuals, and their welfare as data subjects or participants in the market, by concerted enforcement and coherent policymaking by competition, data protection and consumer protection authorities.

The Chairman noted that this potential development raises new questions. For example, should competition authorities consider the level of protection of consumer data as an element of economic performance? Hence, a decline in the level of protection could be viewed as an implicit increase in price. Further, would a weakening of this protection, in itself, be an antitrust problem? In addition, could a violation of data protection law be a violation of competition law? Should competition authorities be concerned with the effect of a merger on data protection? Should competition authorities try to complement weak or deficient consumer data protection regulation or enforcement? These questions were raised as being relevant to the roundtable discussion.

The Chairman noted that the Competition Committee has already looked at some of these issues in three previous roundtables: the hearing on big data in 2016 and the roundtables on quality considerations in zero-price markets and non-price effects of mergers in 2018. The hearing on big data looked at whether access to data could potentially confer market power (that is, data as a barrier to entry). The 2018 roundtables considered whether the level of privacy offered by firms could be an element of quality on which firms compete.

The Chairman noted that the topic attracted quite a number of contributions: 19 in total, 12 from OECD members, four from OECD participants, and one each from Business at OECD, BEUC (the European association of consumer organisations) and TUAC (the Trade Union Advisory Committee to the OECD). He then introduced the experts and thanked them for their taped interventions, which were posted on the roundtable website in advance:

- Ms. Elizabeth Denham, the United Kingdom's Information Commissioner (head of the UK Information Commissioner's Office (ICO)) and Chair of the Global Privacy Assembly. In her video, she highlighted the importance of co-operation between competition and data protection authorities, especially for building consumer trust, assessing the potential impacts of mergers and implementing data portability.
- Professor Wolfgang Kerber, Professor of Economics at the University of Marburg, specialising in competition and data, especially involving the Internet of Things. His video contribution covered issues like data governance and competition drawing on his research on connected cars. He also argued that competition law and privacy issues should be considered simultaneously.
- Professor Alessandro Acquisti, Professor of Information Technology and Public Policy at Carnegie Mellon University, specialising in the economics of privacy. His video focused on research on consumer behaviour towards, and valuations of, privacy.

The roundtable discussion comprised three parts:

1. **Competition assessments**: how to deal with privacy and data protection policies in assessing competition matters.
2. **Competition remedies**: how to devise competition remedies to ensure they do not undermine privacy and data protection outcomes.
3. **Policy development**: how to promote competition in designing and implementing consumer data rights, and how to develop policies that jointly promote competition, privacy and data protection, as well as consumer protection, with respect to consumer data.

The Chair gave the experts the opportunity to commence the roundtable by highlighting what they see as the most important message that they wanted to deliver.

- **Ms. Elizabeth Denham** noted that privacy has historically been overlooked in competition analysis, including mergers, but because of our increasingly data-driven world, competition and data protection must pull together to further the interests of individuals – particularly, autonomy and choice.
- **Professor Wolfgang Kerber** noted that in the digital economy the relationship between competition law and data protection law is very complex with interplays between market failures, enforcement practices and remedies. This requires deep analysis and much more co-ordination between policy areas.
- **Professor Alessandro Acquisti** noted that there is ample empirical evidence of consumers caring for and actually trying to take steps to protect their privacy online.

There is also ample evidence of hurdles and barriers, which can impair privacy seeking behaviour, from asymmetric information to boundary rationality. Therefore, he noted, market outcomes regarding privacy do not necessarily capture actual consumer preferences.

Part I: Competition assessments

Part I focussed on how competition authorities, in their enforcement activities, consider privacy and data protection issues. The **Chairman** noted Wolfgang Kerber's suggestion that instead of deferring the issue of privacy to data protection authorities, competition agencies need to consider market failures regarding behavioural and information problems that may undermine the effectiveness of data protection policies alongside their assessment of potential competition issues. The Chairman noted that the first part of the Roundtable would aim to hear delegate views on this issue.

The discussion commenced with an intervention from the **United States**. The contribution from the United States stated (OECD, 2020[2]):

> *Consumer data rights and competition law serve distinct policy goals, and are often protected by different rules and enforcement functions. Because policy makers besides antitrust authorities may seek to promote diverse goals through data policy, we suggest that policy makers contemplating new or amended consumer data rights also consider the likely impact of proposals on competition and other pro-competitive goals like innovation. Antitrust enforcers should be aware of the effects of privacy legislation on markets they assess for competitive harms, and should take the same into account when assessing the likely efficacy and efficiency of remedies to anticompetitive transactions or conduct.*

The **United States** noted that the Federal Trade Commission (FTC) enforces both privacy law and competition, so it is experienced in these issues. The US economy is data driven and consumer data are important inputs and outputs for many goods and services, so data rights may affect competition in some markets. For example, in the FTC's 2018 case against Core Logic, its view was that the accumulation of historical data was a barrier to entry and the settlement addressed this competitive concern by requiring Core Logic to license data to a third-party entrant.

In some markets, privacy may be relevant to antitrust analysis as an aspect of quality. That is, as a non-price dimension on which firms compete, which may be threatened by a merger or other conduct. However, assessing objectively how much consumers value privacy and what the market dynamics are around it is not a simple task.

The United States argued that the interplay between competition and privacy does not mean that competition and privacy laws should merge. Each of these regimes serve distinct goals; they employ different remedies and their interaction is complex and context specific. Stronger consumer data rights may promote competition, for example, by reducing information asymmetries or limiting exclusionary conduct. However, privacy and competition can also be in tension, creating unavoidable trade-offs. For example, requiring a firm to share data or to allow competitors to access data on its platform may promote competition but reduce privacy. Similarly, laws protecting privacy may undermine competition by entrenching incumbents and raising costs for small and medium sized enterprises (SMEs). Therefore, while privacy can be relevant to competition law, it should not become an independent goal of antitrust. Allowing it to do so, argued the United States, would lead to incoherence that could undermine both privacy and competition. Finally, it was argued that merger control, while it may present a practical opportunity to achieve any

number of ends, is no more a place for enforcing privacy law than it is for environmental law or labour law or any number of other ends that the State might want to achieve.

The US Department of Justice (DOJ) also provided an overview of its experiences. Like the FTC, the DOJ has been examining how consumers might be the victim of anticompetitive harm when digital platforms take more of their data but fail to compensate them with services of additional value. One of the most important markets where that dynamic is at play is in digital advertising. The DOJ has a long history of investigating and prosecuting antitrust violations in ad-supported markets, but never before has individual level data been such an important input to ad-supported business models. To understand the competitive dynamics at play in ad-supported markets, the DOJ held a public workshop in early 2019. During the workshop, industry participants and scholars discussed how businesses collect and monetise data insights, and highlighted that while the collection or sharing of data by third parties is often maligned for its privacy implications, it can be an important tool for disciplining incumbents and providing competitive checks in ad-supported ecosystems. Third-party cookies on websites, for example, can ensure that there are multiple sources of data on consumer interactions with a website (which may be useful for targeted advertising), and can be used by analytics firms to track the effectiveness of online advertising. The ability to measure return on investment in advertising can be an important way to spur competition among sources of advertising inventory.

Antitrust enforcers have also relied on third parties when designing remedies to restore competition. The DOJ recently required data sharing as part of its remedy in the CVS Aetna merger. Licensing of software built on data insights has been another remedy in cases like Google ITA. In the policy quest for an optimal level of data rights and defaults to privacy, agencies must consider whether a consumer expressed any intent about their privacy preferences, or if there is any way to discern or measure consumer intent to share data with one party but not another or to share data for some purposes but not others. Keeping data from third parties may stifle competition and thus reduce consumer welfare without improving consumer outcomes meaningfully along the metric of privacy.

Business at OECD (BIAC) then took the floor. BIAC noted its strong view that although competition and privacy and data protection regimes have distinct policy objectives, these two policy areas need to be co-ordinated closely. There is a real need for regulators in both areas to co-ordinate with each other, especially as the different goals of the two regimes, while being focussed on consumer outcomes, can pull in different directions. Competition law protects consumers by ensuring a vibrant competitive process rooted in the idea that competitive markets are central to investment, efficiency, innovation and growth. It therefore seeks to empower consumers, viewing consumer choice as paramount; while privacy and consumer protection laws focus on individual harms from unfair or exploitive practices. These different ways of looking at consumer welfare do not necessarily put the two regimes into conflict, but they can invoke distinct public policy considerations. In order to be effective, BIAC believes the two regimes should respect rather than ignore their differences.

BIAC was also concerned that an overlapping regime could risk chilling the innovative use of data by businesses. There are many benefits from the collection and use of data by businesses, not just for efficiency and innovation purposes, but also benefits to consumers in the form of more relevant products and services, at a lower (or even zero) price. Overlapping regulation could have a chilling effect on firms' willingness to invest and expand in a jurisdiction, and hence, BIAC argued against overlap and for regulatory clarity (since a lack of regulatory clarity may also have a chilling effect on investment). Competition enforcement decisions can be difficult for other firms to apply to their unique circumstances, especially in innovative industries such as e-commerce, social media and

fintech, which are growing in size and significance in the global economy. Business at OECD concluded that co-ordination of regulatory enforcement is key to ensuring that innovation and investment can continue to flourish without compromising competition or data protection.

Noting the Bundeskartellamt's ongoing case against Facebook, the **Chairman** then turned to Germany.

Germany agreed with the United States that competition and privacy law should not be merged, and noted that the Bundeskartellamt is not a privacy agency. However, it also noted that competition law and privacy law, through data-driven business models, are entwined in a way that it is very difficult to separate clearly in cases where data is the key driver of the dominance of the company, and where data may be subject to remedies in such a case. In relation to the case against Facebook, access to personal data is a key factor in assessing the dominance of a company (alongside network effects). This is reflected in German competition law, which says: *"when assessing dominance, a key and relevant factor is access to data."* Hence, Germany continued, if a "super dominant" company systemically violates privacy principles as part of its business model, how these super dominant companies have gathered and processed all this data is a relevant consideration for competition authorities. This is the core of the Facebook proceeding that the Bundeskartellamt commenced in 2019. The problem was not with Facebook gathering data on Facebook itself, which most users are aware of, but that Facebook also collects consumer data from third-party platforms, and then stores all that data in one user account on Facebook. Further, the user has no possibility, no way to steer the collection of data, because to use Facebook requires a user to agree to the collection of their data on third-party platforms. In this way, data collection and competition law are entwined. Competition agencies, Germany argued, need a certain parameter to assess if the dominant company is dealing with consumer data correctly or not. In doing so, and in the German context, the European General Data Protection Regulation (GDPR) is what policymakers have agreed to in terms of the correct use of consumer data, and hence, it is a relevant consideration in assessing whether a dominant firm has abused its dominance in this regard. Regarding remedies, these were also data-driven to restrict the possibility of Facebook to collect all this data. The case was lost before the higher regional court in a preliminary proceeding. The Bundeskartellamt appealed this, and the Federal Supreme Court will have an oral hearing on the 23rd of June 2020. While the legislator and the agencies can take the case in a certain direction, the court will ultimately take the decision[1].

Next, **Japan** presented its recent work on digital platforms and recent consideration by the Japan Fair Trade Commission (JFTC) on the extent to which abuse of dependency or abuse of superior bargaining position, rather than abuse of dominance, could be a useful tool to solve some of the interactions between competition and data protection.

First, Japan noted increasing concern regarding the use of consumer data by digital platforms. This led the JFTC to convene a study group and conduct 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. 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

[1] In June 2020 the Federal Court of Justice annulled the interim decision handed down by the Higher Regional Court. Afterwards, the case has been referred back to the Düsseldorf Higher Regional Court for the main appeal proceeding. After an oral hearing in March 2021 the Higher Regional Court has referred the Facebook case to the Court of Justice of the European Union for a formal interpretation of the European Regulations at stake. The proceeding is still pending.

bargaining position (ASBP) under the AMA. The guidelines point out that if a digital platform disadvantages or hurts consumers by abusing a superior bargaining position, such conduct will not only impede the free and independent choice of consumers, it will also likely to give the platform a competitive advantage. 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.

Japan then explained the relationship between the ASBP provisions, and the Japanese personal data protection law (the PPI Act). These differ in terms of both purpose and coverage. If a company uses or collects personal information without an individual's consent, which is a PPI Act violation, the personal information protection committee (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. The JFTC co-operates with the PPC to tackle cases regarding digital platforms and consumers as necessary.

The **Chairman** then turned to the experts to respond, starting with **Wolfgang Kerber**. Professor Kerber noted that there are very different concepts of privacy protection between the United States and the European Union. Privacy is a fundamental right in the European Union. In contrast, in the United States' written contribution, they emphasise that there might be a trade-off between the advantages of the data economy and innovation and efficiency also. That is, there is a kind of tension between privacy protection on one hand and innovation and economic efficiency on the other hand. This might also lead to a different relationship between competition policy and law, and data protection and privacy policy and law, between the United States and the European Union.

The other important difference, noted Professor Kerber, is whether it is a task of competition policy to protect consumers against the negative redistributive effects of market power on the welfare of consumers, and this is about the question of exploitative abuse. Again, he noted that there is a huge difference between the United States and the European Union in this respect. From the German and Japanese interventions, and the European Union more generally, such exploitative appeals are captured under competition law. In Japan, it is about superior bargaining power, and this is also a key idea in the Facebook case of the Bundeskartellamt, because it was really a case about abuse, and the question of whether market power might lead to negative effects on privacy is then directly a concern of competition law. However, the difficulty is determining what benchmark to use regarding an abuse of dominance in respect of consumer data. Professor Kerber argued that using a violation of the GDPR as a benchmark for exploitative abuse in competition law does not fit very well in the competition law rationale, because the GDPR only provides a minimum standard for privacy protection, which may differ from what effective competition would lead to.

Professor Kerber also advocated that competition authorities take into consideration market failures in respect of data protection and privacy, and consider these in developing remedies. He argued for greater collaboration between data protection authorities and competition authorities. Regarding the Bundeskartellamt's case against Facebook, he noted that he would have liked to see a parallel case taken by the relevant data protection authorities, with a co-ordinated finding, being a joint solution for solving this problem of two market failures. It would not have to be a joint investigation or a joint proceeding, but the key would be to finding an optimal combination of remedies.

Ms. Elizabeth Denham then intervened on the topic of collaboration and co-operation between competition authorities and data protection authorities. She noted that these agencies are different, and a significant portion of her work is about protecting fundamental rights and freedoms that do not affect competition. For example, the use of facial recognition technology by police forces has nothing to do with the private sector and competition. However, there's a Venn diagram where there is an overlap in the interests and work of competition and data protection authorities, particularly in respect of consumer protection, and things like fairness and transparency and data protection by design, that lead to empowered and informed consumers.

She noted that greater collaboration and co-operation is relatively new. Some 18 months or two years ago, Ms. Denham noted that she did not follow closely the work of the UK Competition and Markets Authority (CMA). However, a formal governance structure now brings the CEOs of the CMA, Ofcom (the media and communications regulator) and the ICO together for four meetings a year, leading a joint work program, because the intersections are growing stronger. One example of collaboration is in respect of digital advertising. The ICO launched an inquiry into the use of personal data in the practice of real-time bidding in online advertising. It convened a roundtable and wrote a report on the risk to data protection in the current ecosystem and the practice of real-time bidding. It paused this work because the CMA launched a market study on digital advertising. The ICO is now co-operating on some of the research for this. Regarding digital advertising, Ms. Denham also noted that in considering the GDPR impacts of real-time bidding, her adjudication in that case might have had the unintended consequence of entrenching the big players in that market. In her role as Information Commissioner, she is required under UK law to have regard for innovation and the digital economy. Hence, the law requires her to take account of the impact of her remedies, sanctions and adjudications in these respects.

Germany then intervened to mention two things. First, that the Bundeskartellamt is in close co-operation with privacy agencies in Germany. There are several privacy agencies in Germany at both the federal level and the regional level. While the Bundeskartellamt did not have a formal green light from these agencies for the Facebook case, it had an informal green light. Second, Germany stated that, if you have a "super dominant" company that forces the consumer to hand over data, day by day, and thus infringe GDPR systemically, thus strengthening its dominance, day by day, by infringing GDPR, it seems quite odd if a competition agency is not able to look at how this dominant company is gathering that data. If the law obliges the competition authority to deal with that question, there has to be a parameter for how to do that, and the parameter, in the case of Germany, it was argued, can only be the GDPR.

Professor Alessandro Acquisti then provided some comments on the issue of consumer attitudes, behaviour and valuations of privacy. Professor Acquisti started by discussing the meaning of privacy. On one hand, there is the dominant definition of privacy from the Alan Wasting days, which is privacy as control over personal information, privacy as protection of information. Then there is the work of the American social psychologist Erwin Altman who refers to privacy as a process of boundary management rather than being monolithically about protection. Altman saw privacy as this dynamic, dialectic process of opening and closing the self to others. This distinction has huge practical implications because, first, there is ample evidence of privacy seeking behaviour by consumers online. There is evidence from surveys of behaviour, field studies, and lab experiments. Just to mention a few: a Pew study from 2013 found that 86% of American respondents had taken at least some steps to protect their privacy online: either to clean cookies, encrypt email, avoid using names in certain forums, or using virtual private networks (VPNs). A study in 2017 found nearly half of the respondents had been using private browsing. A study by academics in 2017 found that 93% of Facebook users have changed the default settings on

their profiles to make their posting less visible and no longer publicly visible. Moreover, the evidence of privacy seeking behaviour is so incredibly widespread that it almost goes unnoticed. For example, people:

- selectively choose whether to reply all or to reply only to certain people in online communications
- use different email accounts to compartmentalise professional and personal lives
- decide whether to use videos when on video calls or conferences.

People engage in this boundary negotiation all the time. However, there is also clear evidence of disclosure and sharing behaviour. Erwin Altman explains that one reason why there is this seemingly contradictory evidence is that people want to manage the boundaries between public and private. So they try to be public in certain instances, they try to be private in others. This might suggest that we have no problem because consumers are able to choose where to set the boundaries to manage their privacy online. However, there is a second set of problems, which explains the contradictory evidence around privacy seeking behaviour and disclosure. There are demand side problems or barriers, or hurdles, which make it difficult for consumers to manage the boundaries of their personal lives online. By properly managed, this means a consumer's ability to achieve their desired combination of sharing and protecting behaviour. These problems from the demand side include asymmetric information, not having a fair knowledge of when data is captured, by whom and how it is used, problems of bi-directionality, and problems related to heuristics and cognitive behavioural biases such as, for instance, hyperbolic discounting. In addition to that, there are supply side problems, which exacerbate demand side problems such as lock-in, network externalities, switching costs as well as platforms intentionally using consumer psychology to nudge users towards more disclosure. Hence, concluded Professor Acquisti, competition authorities and privacy authorities should not consider market outcomes as necessarily capturing consumers' true underlying privacy preferences.

Part II: Competition remedies

The second part of the roundtable focussed on competition remedies in competition cases involving consumer data. This is an important consideration since some pro-competitive remedies may clash directly with privacy or data protection objectives.

Part II started with an intervention from the **United Kingdom**, who in its written contribution talked about a number of potential remedies for problems that the CMA has identified in relation to digital advertising and online platforms. The United Kingdom noted that it viewed data access and interoperability measures as complementary measures, as part of a whole package of options. It also supported Professor Acquisti's observation that consumers are not necessarily able to exert the sort of control that they would like to have over their personal data, including due of nudging techniques employed by businesses.

Regarding remedies, the United Kingdom has tended to think of data access remedies as a particular remedy to address data silos. For example, Google's click and query data. Regarding interoperability, the United Kingdom has tended to view this as a way to balance network effects. These two issues engage data protection issues in different ways. In general, competition and data protection regimes are potentially in tension but in many ways, they are not. For example, regarding consumer empowerment, data protection can improve consumer empowerment and this drives competition. Therefore, there is a strong synergy there on the consumer side.

Where there are tensions, there may be ways to minimise these. For example, for a data access remedy, there may be a way of getting the valuable data for competition, but removing the personal data elements through aggregation or anonymisation or some other mechanism. On interoperability, a key issue is whether those measures are consumer-led. If so, it is much easier to comply with the data protection principles of consent, as a particular lawful basis of processing. The question generally, then, is how you ensure that consumers can exercise control and consent. Further, if you do have these measures, they need to operate in a competitively neutral way. Regarding the "ad tech stack", consent works very well as, potentially, a basis for processing, but it should not operate to give an advantage to the incumbents compared to other players, when substantively there is not really a significant difference in what they are doing. So competitive neutrality is an important principle. There needs to be further discussion on how to achieve it and how to balance those trade-offs. Such discussions benefit from involvement from the data protection authorities, such as the ICO in the UK.

Canada then discussed the trade-offs it has considered in developing competition remedies that do not undermine privacy. The central piece of relevant jurisprudence in Canadian competition law comes from the Toronto Real Estate Board (TREB) abusive abuse of dominance case. This involved an association of real estate agents that instituted rules to prevent its members from broadly using and disclosing online, via virtual office websites, certain information it controlled, including its historical sales data online (e.g. past selling prices of houses). The Canadian Commissioner of Competition brought this case before the Competition Tribunal alleging that these restrictions negatively affected competition and constituted an abuse of dominance. One of TREB's main justifications for their conduct was to comply with its obligations under Canadian consumer privacy laws. However, the Tribunal was not persuaded by this since TREB already allowed its 40 000 members to share this same information, such as past sales data, with their clients through other means (e.g., by fax or by email), among other reasons. Ultimately, the Tribunal agreed with the Commissioner that TREB's rules constituted an abuse of dominance, and ordered TREB to remove those rules. The Tribunal's conclusions in this case do not necessarily support a broader principle that consumer privacy interests can never be relevant to decisions under Canadian competition law; rather, the Tribunal considered that in this specific instance, the privacy argument was an "afterthought", a "pretext", used to justify anticompetitive restrictions.

On appeal, the Canadian Federal Court of Appeal found that business conduct that negatively affects competition but is required to comply with other laws and regulations, such as consumer protection laws, might not breach competition law. Hence, in designing remedies, as well as more broadly, the Competition Bureau may be required to consider the effect that impugned conduct can have on issues like consumer privacy and other data rights more broadly.

Brazil then talked about some of the cases that have arisen in its jurisdiction. In its written contribution, Brazil made the point that that *"fostering competition by stimulating an increase in data sharing does not necessarily occur at the expense of consumer privacy"* (OECD, 2020[3]). It discussed the Bradesco case to illustrate this. Bradesco, a large Brazilian bank introduced two-factor authentication as an additional step for its clients logging into their checking accounts (as opposed to solely when confirming transactions). It was alleged that this practice was intended to deny Guiabolso, a fintech providing personal finance management services, access to client data (which it otherwise obtains by scanning data from users' checking accounts with their informed consent). Having found the conduct to be anti-competitive, CADE (Brazil's Administrative Council for Economic Defense) found itself in the difficult situation of devising a potential remedy. During the investigation, CADE found out that Bradesco has continuously refused to negotiate the

development of an application programming interface (API) to enable data sharing with Guiabolso (despite doing so for a company in a market unrelated to financial services). Hence, CADE imposed a duty to share data, which Bradesco could implement through an API to connect its data warehouses with those of the fintech with the consent of the common clients. To develop the technical aspects of the API further, co-operation with the Brazilian central bank would be extremely valuable. In addition, it could be aligned with the new regulation of Open Banking Brazil, which was just released and is expected to be fully effective by the end of 2021.

Egypt then spoke about using data portability as a remedy for a merger between two ride-sharing platforms. Specifically, the Egyptian Competition Authority (ECA) required data remedies, including data portability, when issuing a decision concerning Uber's acquisition of Careem. Uber and Careem are the two largest ride-sharing platforms in the region. 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.

The ECA 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 port their data to alternative ride sharing service providers. One of the main hurdles faced by the ECA was trying to achieve interoperability between platforms, which poses technical challenges. In the absence of interoperability, the ECA had Uber commit to allow users to download their data in a common format and use its best efforts to co-operate with other ride sharing service providers. The ECA noted the role of co-operation between competition authorities and data protection authorities in devising remedies, and the importance of increasing digital awareness to foster greater competition.

The **Chairman** then turned to the experts to add their views on remedies, starting with **Ms. Elizabeth Denham**, to which he asked about the United Kingdom's experience in co-operating on remedies across the various agencies. Ms. Denham noted that in addition to the formal co-operation frameworks noted earlier, secondments are a way to facilitate greater inter-agency co-operation. In particular, the ICO is currently seeking secondments from economists to help it understand the impact of its remedies and decisions. For example, the UK Parliament has just approved an age-appropriate design code to ensure privacy by design for services directed at children, which requires the ICO to provide an economic analysis of the impact of its 15 design requirements. Co-operation between data protection authorities and competition authorities is at various levels of maturity across the world. In some countries, the dialogue has not yet started, but it is mature in the United Kingdom.

Regarding areas where co-operation is important, Ms. Denham highlighted mergers and acquisitions, noting that competition authorities have been slow to come to the table to look at acquisitions where the most important asset in a merger is the data sets. She noted that this was the case in 2016, with the Facebook/WhatsApp case, and the ICO intervened as a data protection authority because it did not see that there was a legal basis for WhatsApp to share its data with its new parent company, which was Facebook. The ICO ultimately required WhatsApp to sign an undertaking that they would not share those data sets until

they could prove that they had the legal authority to do so. Ms. Denham further noted that thinking about data as an asset in mergers and acquisitions is an important new area of research and co-operation. However, it is difficult to put some kind of a value on data in an acquisition as data protection and data is so context specific. This requires further work and co-operation. As a data protection authority, the ICO has to make judgment calls on what is reasonable and what is fair in a given circumstance. In the same way, competition authorities will be better at analysing and assessing the quantitative value of data if they work with data protection authorities and apply what has been learnt from valuing other intangibles such as "good will". Ms. Denham also noted that there could be benefit from giving data protection and competition authorities the power to intervene in the other's cases, where this in the public interest.

Last, Ms. Denham noted the need to tackle hidden processing of data. She noted that the ICO has worked to "look under the bonnet", to explain to consumers these complex ecosystems where their data is processed. Not only do agencies have to consider consumer attitudes and behaviours online, they also need to educate them about these complicated ecosystems. For example, the ICO did this in looking at Cambridge Analytica, the sharing of voters' data online, and the nudges and behaviour changes in that context. She stressed that it is critically important that data protection authorities keep showing consumers and individuals how their data is processed online. Such work is ongoing on digital advertising.

The **Chairman** then asked Professor Wolfgang Kerber a question on behalf of Sweden: given the amount of data that is collected, is there a risk that sharing data could enable firms to deduct information about the market strategies of the competitors, or can we safely assume that sharing of consumer data will not facilitate collusion?

Professor Kerber said that this depends on what type of consumer data is being shared. For example, providing access to certain information such as energy consumption data or technical data in a connected car that monitors components for remote diagnostics or remote maintenance services, would be unlikely to facilitate collusion. These data do not allow any conclusions to be drawn about the business strategies of competitors. However, this might be very different if, for example, data about buying histories of consumers were shared because this can include transaction data. If such data included data about prices, quantities and rebates, for example, and if such consumer transaction data are mutually shared within an industry, then this might work like a traditional market information system, which allows firms to mutually monitor each other and this can also stabilise price collusion. So it depends what kind of consumer data is being shared, and this shows again the importance of analysing very specifically what kind of data are shared, in what way, and with whom.

Professor Alessandro Acquisti then noted that any policy approach that relies on consumers taking responsibility for their own data protection is likely to fail. He stressed that there is so much empirical evidence now that notice and consent regimes are not sufficient, and transparency and control are necessary but not sufficient conditions for consumers' ability to manage their privacy online. One of the studies he mentioned earlier, in which half of the respondents were using private browsing, also found that two thirds of the users actually misunderstood what private browsing was actually doing. They thought it was giving much more protection than what it actually was giving them. Similarly, in the study, which found that 93% of Facebook users now change their default settings to make their posts less visible, while users moved towards greater privacy, Facebook in fact shared their data with more and more third parties. The modern consumer, when it comes to privacy, has to continuously find new ways to protect and manage their privacy when the challenges keep expanding and changing and growing. Professor Acquisti noted that it is

unfeasible and unfair. If the goal of policy makers is to protect privacy, reliance on any tool that puts too much weight on notice and consent is not going to work, he argued.

The **United States** responded to Professor Acquisti noting that while consumers engage in a range of behaviours where they do not fully understand what is going on with their data, and even if there is evidence to support the proposition that the market isn't fully reflecting what consumers want, that does not mean that policy makers better understand consumers' preferences. Further, the United States cautioned against allowing a belief that there may be unrevealed preferences in the market to lead to the conclusion that there has been an exercise of market power. Instead, it argued that competition agencies should continue to adhere to the evidence that they find, and in the absence of such evidence, should be very careful about allowing other values, however important, to become matters for competition policy and enforcement. Privacy can be relevant, the United States noted, but competition agencies need to assess this on a case-by-case basis.

Professor Alessandro Acquisti agreed with the concerns raised by the United States, and noted the importance of interpreting data carefully. Professor Acquisti referenced the work of Erwin Altman, who talks about desired privacy as compared with realised privacy. That is, what consumers want and what they can achieve. In the market, there could be over or under delivery of privacy. That is, it could be that consumers achieve less privacy than they want, or have more privacy than they want. At least in theory, the fact that we have asymmetries: information asymmetries, rationalities, biases, does not itself tell us whether there is too much or too little privacy. However, Professor Acquisti argued that once you add the survey evidence and you consider the supply side practices that nudge consumers towards more disclosure, then this suggests the market is under delivering on privacy. In other words, Professor Acquisti believes that realised privacy in the marketplace is probably less than desired privacy.

Part III: Policy development

The third part of the discussion was on co-operation in developing policies regarding consumer data rights and competition.

The discussion started with **Italy**, who has undertaken a multi-disciplinary approach, involving the competition agency, the communications regulator and data protection agencies, in its recent study on big data. Its view was that the complexity of the issues at stake when consumer data rights are relevant requires not only antitrust enforcement but also adequate advocacy in order to contribute to the definition of an appropriate regulatory framework. Starting from three different 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 highlighted 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 Italian Competition Authority. Almost 93% of the interviewed users declared to be interested in their privacy protection, but only one third of them denies consent to the collection and utilisation of their data. In relation to consumer data rights, the three authorities have 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.

Spain was next to take the floor. Its written contribution called for deeper co-operation between the authorities and institutions that are involved in regulation in this area, and raised the concern that horizontal regulation may have limitations to address some types of competition issues. However, it noted that policy makers should consider the need for sector-specific regulation on a case-by-case basis. For example, data portability would appear to be procompetitive in the sharing economy. For fintech, principles of open banking, technical neutrality and interoperability, are relevant. Now Spain is looking at what should apply in the case of online advertising. It also noted the European wide debates on this issue. Spain's experience has highlighted two things. First, there is a need to combine instruments: horizontal regulations, sector regulation, and competition advocacy for a good regulation, as well as competition enforcement, depending on the case. Second, the degree of technical complexity is very high. Hence, there needs to be a multi-faceted approach and a multidisciplinary approach, combining the expertise of different agencies. As the Spanish Competition Authority is also the main a sectoral regulator for the regulated industries, it benefits from a diversity of views and skills.

Regarding possible shortcomings with horizontal regulations, Spain noted that enforcing privacy and consumer data protection and mandating consumer consent can distort competition and can benefit the big players who are more capable of getting that consent and of accessing data. Hence, Spain noted its preference for sectoral approaches that combine all the instruments depending on the case. For instance, while data portability may be a good idea in the payment sectors it might not be optimal in other sectors. Spain advocated for administrative co-operation between agencies and the need to be equipped to deal with some with these complex challenges. Having the telecom regulator and the competition agency in the same house means there is a decent exchange of views regarding remedies for enforcement in complex cases regarding the definition of market power, of access obligations, of interoperability and of the appropriate remedies to balance competition, innovation and investment.

Next, the **Chairman** asked the European Commission for its views on whether Europe's General Data Protection Regulation (GDPR) may be a limited instrument and whether sharper tools might be required.

The **European Commission** noted that the GDPR is a legislative framework for a fundamental right. This remains the case even if all the specific rights granted to the data subjects have to come with obligations on companies in order to make them effective. Given this, the European Commission noted that there is a clear case for strong horizontal legislation, and that the GDPR imposes minimum safeguards for protecting the rights of data subjects. That said, the European Commission is also looking into areas where more targeted legislation may be needed. For example, to address issues of data access and portability. The need for such legislation would need to be identified not only based on the market structure as others have noted but also according to the types and the uses of the data concerned. Such instruments would need to interact with the basic rules, not replace or supersede them. For example, in the Payment Services Directive (PSD) there is an obligation to make data accessible to providers of certain defined services to open up competition and innovative services, and that is dependent on the specific intent of the customer, again in line with basic data protection rules.

As the European Commission detailed in its written contribution, Article 20 of the GDPR provides for a strong basic portfolio right, but further elaboration is needed not only in the form of innovative technological solutions which will take place partly in the private sector and partly with public stimulation, but also in selected areas with sector-specific rules. The

European Commission's data strategy, which is still in its infancy in terms of specifics, highlights the possibility to design specific rules for, just to give one example, who can access and use machine generated consumer data coming from the use of Internet of Things (IoT) applications like smart home appliances or wearables. As another example, the data strategy envisions the creation of European "data spaces" for key sectors and some of these might include specific rules on access and portability. One candidate mentioned in the strategy document is consumer health data. In in this field as in others, policy makers would have to design the rules in a way to minimise lock-in effects and promote the portability of data, including across the borders of member states.

The European Commission, noting Ms. Elizabeth Denham's comments in her video introduction on the webpage, also highlighted that data portability will be more effective in preventing lock-in if the market structure in question is such that there are real alternatives to an incumbent. In order to enhance our ability to address structural problems, and in addition, of course, to continuing active case-by-case enforcement, at the beginning of June the European Commission launched public consultations on two important proposals. One is a "digital services act", including potential ex ante rules for very large online platforms acting as gatekeepers that now set the rules of the game for their users and for competitors. The second is the creation of a new competition tool to address structural competition problems by ordering structural and/or behavioural remedies without the need to find an infringement of the competition rules. Now these have different policy options. One consideration is whether the new competition tool should be limited to digital markets or have a more horizontal application or whether it should apply only to dominant companies or also to non-dominant companies with market power, and what the exact calibration of that should be.

The European Commission is aware of the concern that large platforms can invoke privacy interests as justifications for changes in policy and restrictions on the sharing of data. Such concerns are complex and somewhat preliminary, and of course, a number of data protection authorities (including the Irish data protection authority) are still undertaking a number of investigations into the large platforms, which may affect some of these practices. Hence, data protection law as such may change in the near to medium term. In addition, of course, a competition authority may eventually be tasked with investigating the competitive effects of conduct involving consumer data access restrictions and trying to find a way to promote competition while also protecting privacy.

Next, **Colombia** talked about its experience in using competition advocacy to influence policy making in other spheres. Colombia's competition authority (the SAC) has powers in respect of competition, data protection and consumer protection. The SAC has been involved in competition advocacy which involves i) recognising the relevance of compliance with data protection and consumer protection policies, ii) assessing the possible effects on competition of those proposed policies that involve the regulation of data-driven economic activities, and iii) providing recommendations to help mitigate these effects. It discussed two examples.

- In 2013, the SAC provided comments to the Ministry of Information and Communication Technologies on a draft regulation that contained general requirements and conditions to for postal payment service operators to obtain qualifications, as such the asset and risk mitigation requirements and systems, to manage risk of money laundering and terrorist financing among other things. The SAC acknowledged that one of the key aspects of the project was that it established that postal payment service operators would identify customers using personal information such as contact details, occupation, signature and fingerprints. In this respect, the SAC recommend considering the provisions of the Colombian general

data protection regime. In 2016, the SAC fined a postal payment service operator for failing to adequately inform its consumers that their personal data was going to be used for marketing and advertising proposals outside of the specific commercial relationship. The data protection authority found that the organisation's consent format was not sufficiently clear and precise about the specific means of the collection of personal data, the rights of its consumers as data subjects, and the contact information of the person responsible for processing information that had been provided in the context of a commercial transaction.

- In 2017, the SAC provided comments to the Ministry of Transportation regarding the conditions of interoperability of tolls with electronic vehicle payment collection. The project aimed at establishing the legal, technical and financial conditions between intermediaries and operators allowing users who sign contracts with any intermediary to transit freely through the operators' different tolls, thereby ensuring national interoperability. The operator is responsible for ensuring the functioning of the electronic tolls and roads, and collecting tolls. On the other hand, the intermediary will have direct contract with the user and will, among others, collect a payment from its customers and provide payment to the toll operators for the use of the road infrastructure. The project proposed to impose several conditions and requirements to obtain certifications for the operator and the intermediary. These circumstances raised competition concerns. The SAC highlighted that it seemed proportionate and reasonable to establish certain requirements to enable the different actors in the system to communicate.

Australia then talked about the implementation of its Consumer Data Right (CDR), which was legislated in August 2019. The CDR was intentionally drafted to cover all consumer data, but its implementation is staged by sector, beginning with the banking sector, then the energy sector. The Australian Competition and Consumer Commission (ACCC) is responsible for developing the rules for the CDR. It is also the delivery agency for providing the technology that supports data sharing and the enforcement of competition rules. The Office of the Australian Information Commissioner for Privacy Regulation also has a role in implementing the CDR, and the two bodies have agreed a joint compliance and enforcement policy to apply together. Both agencies also work closely with the Data Standards Board that develops the data standards and structures for data sharing.

Australia has learnt from the United Kingdom experience of open banking. Namely, that data portability is complex and difficult to implement, which is why there has been a phased approach to the CDR. Under the phased approach, from 1 July 2020, Australia's four major banks will be able to share basic account information for savings and transaction accounts and credit cards for single customers. From 1 November, this will be extended to loans, including home loans, investment loans and mortgage offset accounts, as well as joint accounts, closed accounts and an additional range of APIs for things like direct debits and scheduled payments that are useful for account sharing. From 1 February 2021, banks are due to share data for a wide range of accounts like trust accounts and asset financing facilities. One key issue is security. Because the ACCC will be holding the register with the security keys to facilitate data sharing, there has been discussion about who should be accountable for security across the whole ecosystem. From an international perspective, there may be benefits from increased competition and increased cross-border commerce. However, there are also challenges such as for accreditation, identifying customers, and ensuring that the right privacy protections are in place.

Germany made a short intervention to note that Germany's competition law is under amendment. The proposed amendments include issues relating to data and access to data. One change will be to broaden the essential facilities doctrine, which has been quite narrow

to date, to include access to data. In addition, there will be a change to the law with regard to access to data if there is relative market power, especially if a company has been involved in generating that data. Germany noted that these amendments could raise difficult questions on how GDPR might come into play again if a competition agency is going to grant access to personal data to third parties who need that data in order to be able to compete with larger incumbents. At least as far as Germany is concerned, there is more to come with regards to data and access to data in respect of competition law, policy and enforcement.

The **Chairman** then turned to the experts for any last comments to conclude the Roundtable, starting with Professor Wolfgang Kerber.

Professor Kerber noted Professor Acquisti's comments about the policy approach, saying that he agreed that policymakers should be a bit cautious about data protection and consumer protection policies that rely on the behaviour of consumers. That is, to what extent is it sufficient to give consumers information and make them aware of certain kind of dangers, whether in respect of data sharing or more broadly? Professor Kerber agreed with Professor Acquisti's scepticism in relying on the behaviour of individual consumers to bring good privacy outcomes. He also noted that consumers might have little choice when it comes to privacy. He suggested that policymakers question whether giving consumers information would be sufficient for solving this market failure problem of information and behavioural problems, or whether regulation is required.

The **Chairman** then turned to Ms. Elizabeth Denham for her final thoughts.

Ms. Denham predicted that in the next five years we are going to see competition, consumer protection and data protection being closer and they will be moving in lockstep and that is just the requirement of the digital economy, and the role that data, much of it personal data, plays. She also echoed what Professor Kerber said, that even if policy makers and enforcement agencies try to educate consumers about what happens with their data in an ecosystem, consumers expect that somebody (i.e. the government) "has their back". Consumers assume that there is an authority or authorities out there that are watching, especially some of these big platforms, that have standards for the platforms to follow, that are taking action when there is consumer or data subject, or individual, or market harm, and they cannot be expected to be able to understand exactly what they are consenting to. Ms. Denham concluded that consent is increasingly going to be challenged in the digital world and there is likely to be an increasing role for standards around sound data governance, ethical practices and a more systemic and standards setting view, rather than leaving it to the consumer to consent.

The **Chairman** concluded by thanking the experts, and the countries that contributed to the Roundtable, both as part of the discussion, as well as by providing written contributions. He noted that there are important points of agreement, the first one being on the interaction between the competition and data protection, and the fact that these two policies areas, which have different objectives, may in some cases reinforce each other and in other cases conflict with each other. Second, at the level of policy making there is a tendency for more co-operation, which is important to avoiding conflict. It was very clear that on remedies, in many cases, there could be benefits from a closer exchange between data protection agencies and competition agencies. Where there were differences was on something which was forcefully mentioned by the experts, which is the fact that in this area, consumers may not be able to make the choices that they want to. Therefore, what we do in terms of promoting competition, or even in terms of promoting data protection, may not be enough to allow consumers to really express their preferences as they should be able to.

So then, there are two questions. One is should that be integrated into the analysis of competition authorities and it seems that there was a general feeling in the Roundtable that,

no, it is too early and we do not know enough. We do not want to move away from the "standard analysis", except in some jurisdictions, and certainly, Germany is leading the way in a different direction. The second question is if we start from the idea that behavioural economists have recognised that the choices of consumers are very much biased when it comes to data, what does that mean in terms of the value of competition in terms of promoting the welfare of consumers? In other words, we assume that more competition improves consumer welfare. Is that true in an area where consumers may not be aware of the choices that they could make, that they should make, or even of what their preferences are. There is a bit of a question mark, which may be a good opportunity to revisit this issue and invite our experts back again, when we will have deepened our co-operation between competition authorities and data protection authorities.

References

González Fuster, G., R. van Brakel and P. De Hert (eds.) (2019), *Data Protection and Competition Law: The Dawn of 'Uberprotection'*, Edward Elgar Publishing, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290824. [1]

OECD (2020), *Consumer data rights and competition – Note by Brazil*, https://one.oecd.org/document/DAF/COMP/WD(2020)41/en/pdf. [3]

OECD (2020), *Consumer data rights and competition – Note by the United States*, https://one.oecd.org/document/DAF/COMP/WD(2020)39/en/pdf. [2]