BUSINESSatOECD

Discussion Points

Presented by the *Business at OECD* Competition Committee to the OECD Competition Committee

Consumer Data Rights and Impact of Competition

June 12, 2020

Business at OECD recognizes the increasing importance of consumer data rights and their intersection with competition law and is pleased to have the opportunity to comment on these issues. These comments build on contributions of *Business at OECD* on related subjects, including Personalised Pricing in the Digital Era,[1] Quality Considerations in Digital Zero-Price Markets,[2] and Non-Price Effects of Mergers.[3]

These comments are organized as follows: Section I provides background on the topic and presents the nuanced challenges that decision-makers will face in regard to this topic; Section II explains what consumer data rights are and how they are regulated; Section III reviews the emerging role of data in business; Section IV makes recommendations to the OECD on the intersection of competition law and consumer data rights; and Section V concludes.

I. Introduction

1. The level of collection of consumer data, as well as its value, is unprecedented and growing daily. The Internet and the advent of new technologies in the digital era allow companies "to obtain, track and analyse ever-larger quantities of data regarding their [consumers]."[4] 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

---

[1] *Business at OECD*, Discussion Points Presented by the Business at OECD Competition Committee to the Joint Meeting of the OECD Competition Committee and the OECD Committee on Consumer Policy regarding Personalised Pricing in the Digital Era (Nov. 28, 2018), *available at* http://biac.org/wp-content/uploads/2018/11/BIAC_JCCP_Personalized-Pricing_2018-11-15_FINAL1.pdf [hereinafter *Business at OECD* Personalised Pricing Paper].

[2] *Business at OECD*, Discussion Points Presented by the Business at OECD Competition Committee to the Joint Meeting of the OECD Competition Committee and the OECD Committee on Consumer Policy regarding Quality Considerations in Digital Zero-Price Markets (Nov. 28, 2018), *available at* http://biac.org/wp-content/uploads/2018/11/BIAC_JCCP_Zero-Price-Considerations_2018-11-21_FINAL1.pdf [hereinafter *Business at OECD* Zero-Price Markets Paper].

[3] *Business at OECD*, Discussion Points Presented by the Business at OECD Competition Committee regarding Non-Price Effects of Mergers (June 6, 2018), *available at* http://biac.org/wp-content/uploads/2018/05/BIAC_CC_Non-Price-Effects-of-Mergers_2018-05-22_FINAL1.pdf.

[4] *Business at OECD* Personalised Pricing Paper, *supra* note 1, ¶ 1.

can receive personalized offers for products and services likely to be of most relevance, interest and usefulness to them.

2. 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.[5]

3. 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.

4. 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.

5. *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.

---

[5] Maureen K. Ohlhausen& Alexander P Okuliar, *Competition, Consumer Protection, and* the Right *[Approach]* to Privacy, 80 ANTITRUST L. J. 121, 122 (2015). These issues were discussed in the decision of the Bundeskartellamt regarding Facebook. Bundeskartellamt, Case No. B6-22/16, Decision under Section 32(1) German Competition Act (GWB), Feb. 6, 2019, *available at* https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

II. What Are Consumer Data Rights and How Are They Regulated?

6. In the context of these comments, consumer data rights encompass both privacy rights and the protection and portability of personal data. Consumer data comprises all of the personal, behavioural, demographic and other information that customers actively share or passively leave behind as a result of their Internet use. Data collection and consolidation by companies is typically aimed at generating insights into customer behaviors, such as their buying choices, satisfaction levels, desires and needs. Accordingly consumers derive significant benefits from such data collection in many cases.[6]

7. There are divergent standards for consumer data rights and consumer protection laws around the world. In contrast to competition law, this makes it difficult to speak of one set of principles or norms for consumer data protection. For example, the European Union has taken a strong pro-consumer stance with respect to data rights under the EU's General Data Protection Regulation (GDPR).[7] The United States, on the other hand, promotes consumer data regulation that focuses on the value and integrity of consumer data in the context of commercial interests to a greater degree. But not even this latter approach is monolithic, as evidenced by different approaches in certain of its states.[8]

8. Variances across countries notwithstanding, consumer protection and privacy laws have different goals from those of competition law. Privacy and consumer protection laws deal with the regulation, storing, and use of personally identifiable information, personal healthcare information, financial information and other information. Its policies are aimed at ensuring that personal data and information are protected. Privacy and consumer protection laws are part of a regulatory framework aimed at protecting consumers from individually potential harmful activity. Competition law, in contrast, aims to ensure that market competition is not restricted or undermined in ways that are detrimental to the economic framework. Rooted in the idea that competitive markets are central to investment, efficiency, innovation, and growth, competition law stands for the protection of consumers, the protection of competition, and freedom of competition and economic efficiency. It seeks to empower consumers as well as companies and sees informed consumer choice as paramount.

9. The disparities between the purposes of competition law and consumer protection law does not render their goals inconsistent or mutually exclusive. Both regimes strive to protect and advance consumer welfare. While it follows that they can work together or at least alongside each other to shape a society that is both progressive (through competition) and safe (through privacy regulation), this should be done in a way that respects, rather than ignores, their differing perspectives and goals (which are complementary, not interchangeable).

---

[6] One example of these benefits are location-based services. Certain apps—mapping, delivery, fitness—deliver services tailored to the user's location and would be much less useful if the apps were unable to collect location data. In addition, certain apps may use the location data to offer location-based advertising to the user (which, in turn, may allow the app to be offered for free to consumers).

[7] General Data Protection Regulation, 2016 O.J. (L 119) 1.

[8] States are increasingly regulating consumer data rights. For example, California recently enacted the Consumer Privacy Act, which enforces the first and only set of consumer data privacy protection laws in America. California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100 - 1798.199.

III. What is the Emerging Role of Data in Business?

10. The collection, use and sharing of consumer data is an evolving and highly innovative aspect of the digital economy. The emerging role of data in business develops and builds on itself more each day for the mutual benefit of businesses and consumers. Businesses benefit by enhancing their likelihood of attracting and reaching their target market more accurately and successfully. Consumer data enables businesses to provide new and improved services and products that consumers are more likely to want in customer-customizable fashions. The ads on Facebook, the suggested products on Amazon, and the instructional videos recommended on YouTube are examples of the personalized goods and services that consumers engage with daily in exchange for their data.

11. The consolidation of data across business platforms often creates significant efficiencies and gains in consumer welfare.[9] Such efficiencies and consumer welfare gains underpinned the European Commission and U.S. Department of Justice's decisions to approve Microsoft's search engine venture with Yahoo!, which aimed to make searches faster, more personalized to individual users, and more efficient,[10] as well as the European Commission's decisions in Microsoft's acquisitions of Skype and LinkedIn.[11] Data sharing invites other economically advantageous opportunities as well. Businesses can use consumer data insights to sell advertising, thereby enabling the availability of free products and services. They can also to sell data directly to third parties.

12. One relatively recent development that demonstrates the increasing commoditization and availability of data is the growth of data brokers (among other data suppliers). In 2014, The U.S. Federal Trade Commission (FTC) conducted an in-depth study about data brokers based a sample of nine companies: Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future.[12] The FTC report describes the vast offerings already available from these data brokers, which collect and store billions of data elements covering nearly every U.S. consumer. One of the nine data brokers has 3,000 data segments for nearly every U.S. consumer.[13] Data brokers offer extensive data packages to businesses; Acxiom, for example, offers access to consumer segments for almost every holiday and interest. The proliferation of data brokers in today's consumer data economy illustrates the new and innovative avenues data collection can take and the outputs data can generate.

13. The progress and advantages afforded by commercial data use is not without risks, specifically those related to consumer data rights. Some of the harms associated with businesses relying on

---

9 In addition, data can be an important input in the production of a firm's output. That said, the value of data can only be unlocked when combined with other inputs. Because firms differ in their ability to do this, success is not necessarily a result of the volume of data. Rather, it is the firm's ability to combine the data with other inputs to produce something of value.

10 Ohlhausen & Okuliar, *supra* note 5, at 151.

11 Case COMP/M.6281—Microsoft/Skype, Comm'n Decision (Oct. 7, 2011), *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m6281_924_2.pdf; Case M.8124—Microsoft/LinkedIn, Comm'n Decision (Dec. 6, 2016), *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

12 FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

13 *Id.* at 46-47.

consumer data include discrimination, exploitative pricing, a lack of transparency, and bias perpetuation, which are not necessarily competition issues.[14]

14. In the age of an ever-evolving data economy, regulating consumer data rights has become a moving target, further raising the question of what the role of competition law is and ought to be as it relates to this data economy.

IV. Competition Law and Consumer Data Rights

15. Competition law and consumer data rights are typically regulated under separate regulatory regimes and by separate agencies and authorities. As discussed in Section III, business' access to and use of consumer data can lead to more market efficiencies that benefit consumers (through such means as efficient pricing and effective advertising) and also harm consumers (through such means as discrimination and predatory pricing).

16. This is one area where consumer protection and competition law can be at odds with each other. From a competition law perspective, price discrimination is generally pro-competitive or benign (i.e., increases output).[15] Unlike with uniform pricing, price discrimination enables businesses to expand their marketplace, attract customers that might otherwise not fit their price point, and compete. It is through consumer data collection that companies can generate insights that enable them to be more competitive, which ultimately contributes to a more efficient and competitive marketplace.

17. Conversely, from a consumer law perspective, price discrimination can be harmful if it means that vulnerable customers (such as consumers of a racial minority, low socio-economic status, or old age) pay more, or if the cross-subsidisation is to such a significant extent that consumers are harmed just by having to pay the highest prices. This can be detrimental to the targeted consumers who may not see such products offered at lower prices. Charging certain types of customers higher prices to artificially lower or offset lower prices for other customer groups may create unfair outcomes for consumers both socially and economically.

18. While competition and consumer protection share the objective of consumer welfare, they pursue this objective in different ways. "Competition law seeks to preserve the forces of competition [including product choice] and in doing so ensure firms face pressure to keep prices low, quality high, or to engage in innovation, depending on the specific circumstances of the market."[16] In other words, competition law aims to protect consumers from harm that can arise from market concentration or power that reduces that pressure. Consumer protection, on the other hand, seeks to prevent individual harms to consumers, such as may arise from unfair practices, irrespective of the level of competitive pressure in the marketplace. In the context of consumer data and privacy, individual rights

---

[14] One pervasive example is businesses charging women higher prices than they charge men for the same product based on women's greater willingness to pay as indicated by their prior online behaviours and activities that online platforms have tracked.

[15] *See* OECD, *Personalised Pricing in the Digital Era—Note by the United States* (Nov. 28, 2018), *available at* https://one.oecd.org/document/DAF/COMP/WD(2018)140/en/pdf.

[16] OECD, *Quality Considerations in the Digital Zero-Price Markets—Background Note by the Secretariat* ¶ 121 (Oct. 9, 2018), *available at* https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf [hereinafter OECD Digital Zero-Price Markets Secretariat Note].

(or standards of treatment) can generally be asserted against firms of any size and regardless of market dynamics.

19. The intersection between competition law and consumer data rights can have an impact on competition in markets. To ensure that businesses and consumers obtain maximal benefits from the digital economy, *Business at OECD* recommends: (a) maintaining separate privacy and competition regimes; (b) improving regulatory cooperation amongst privacy and competition authorities; and (c) carefully considering theories of harm regarding consumer data for the purposes of competition law enforcement. Each of these recommendations is discussed further below.

A. Maintain Separate Regimes

20. As the generation, collection and use of data continue to grow, competition law and privacy regimes will continue to develop and overlap.[17] However, regulators and policymakers in both of these regimes should recognize that the overlap between these spheres does not call for a fusion or intertwinement of regulations over them. To best realize the respective mandates of competition law and consumer protection law, their enforcement should remain separate.

21. *Business at OECD* recommends that continued responsibility for enforcing consumer protection and privacy rights remain with consumer protection agencies and privacy commissions. These agencies and commissions should coordinate with competition authorities to ensure that their advocacy and enforcement activities create as much certainty and predictability as possible.[18] Avoiding or minimizing regulatory overlap will reduce unnecessary uncertainty about compliance for consumers and businesses.

22. Traditionally, the litmus test for competition law enforcement has been where intervention is necessary to ensure competition "on the merits" and thereby protect consumer welfare.[19]

23. It is key to "distinguish between privacy-related issues best handled under the competition laws from those best [dealt with] by consumer protection laws or sectoral privacy laws."[20] Consumer protection law in developed regimes is able to manage the consumer harms of data collection. For example, it can be more flexible and better suited than competition law to require transparency remedies. "[W]hereas the consumer protection laws are preoccupied with ensuring the integrity of each specific contractual bargain," competition law is tailored to broader, macroeconomic harms in markets.[21] Indeed, competition law is typically invoked in respect of consumer data in the context of abuse of dominance regimes that seek to address the market power of large firms. By contrast,

---

[17] *Business at OECD* is concerned about the risks associated with ex ante regulation and cautions against the development and implementation of rigid rules that risk sacrificing the efficiencies and other benefits of innovative platforms. *See* Comment of the Global Antitrust Institute, George Mason University School of Law, on the European Commission's Public Consultation on the Regulatory Environment for Platforms ¶ 9 (Dec. 29, 2015), *available at* http://masonlec.org/site/rte_uploads/files/GAI_Comment%20on%20EC%20Platform%20Consultation_12-29-15_FINAL.pdf [hereinafter GAI Comment].

[18] In releasing the *Facebook Decision*, the Bundeskartellamt in its press release emphasized that it had worked closely with the national data protection authority. Press Release, Bundeskartellamt, Bundeskartellamt prohibits Facebook from combining user data from different sources (Feb. 7, 2019), *available at* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[19] *Business at OECD* Zero-Price Markets Paper, *supra* note 2, ¶ 24.

[20] Ohlhausen & Okuliar, *supra* note 5, at 151.

[21] OECD Digital Zero-Price Markets Secretariat Note, *supra* note 16, ¶ 121.

consumer protection and privacy laws should offer consumers protection of their individual rights irrespective of the market power of a firm.

24. Further, tensions that exist between the two regimes could deem competition law ill-fit to address consumer data rights issues. As an example, in zero-price markets funded by advertising, there may be an optimal level of advertising. When advertisements are served, the market will be operating most efficiently when they are targeted in the most relevant possible way. As *Business at OECD* has previously explained, "[t]o the extent a society seeks to protect users from targeted advertisements, this goal is better achieved on its own terms, rather than by trying to adapt competition law analysis, especially against conduct that could otherwise be accretive to consumer welfare."[22] As compared to competition law, consumer protection would also be a better means to protect consumers from inaccurate or misleading advertisements. It should not presumptively diagnose misleading ads as a symptom of a competitive imbalance but instead aim to create measures that proactively prevent consumer manipulation—a protective measure that fits squarely within the mandate of consumer protection.[23]

25. Previous decisions support each of these authorities governing only within their own regimes, particularly when it comes to remedies or enforcement measures. For example, "the U.S. Federal Trade Commission's decision in *Google/DoubleClick* and the European Commission decision in *Facebook/WhatsApp* . . . emphasised that competition authorities are not data protection authorities."[24] Indeed, only 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, should traditional forms of competition enforcement be deployed to address such market failures.

26. Not only do the competition and consumer protection law regimes each have their own roles responsibilities, but also their own principles, values, and goals.

27. *Business at OECD* recommends that competition law should only be triggered when the issues at stake—including privacy—directly touch market competition. Privacy has been considered in a limited number of cases in the competition assessment of a transaction, including in the *Microsoft/Skype* and *Microsoft/LinkedIn* mergers as well as the German Facebook investigation.[25] In *Microsoft/LinkedIn*, the European Commission considered whether the merger restricted competition in relation to privacy protection in the market for professional social network services.[26] To the extent that privacy is a parameter of competition, then competition law is already able to address the harm that can arise from a reduction of competition on quality parameters. In such circumstances, enforcement to avoid that reduction may be more effective than regulation. Competition and consumer law can be used as complementary corrective devices to address information asymmetries that data protection law cannot alone address. "Competition authorities' investigations reveal that privacy can be an important parameter of competition and [potentially] a driver of customer choice in

---

[22] *Business at OECD* Zero-Price Markets Paper, *supra* note 2, ¶ 27.

[23] *Id.* ¶ 29.

[24] OECD Digital Zero-Price Markets Secretariat Note, *supra* note 16, ¶ 78 (international cites omitted).

[25] *Id.* (citing Case COMP/M.6281—Microsoft/Skype, Comm'n Decision (Oct. 7, 2011), *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m6281_924_2.pdf; Case M.8124—Microsoft/LinkedIn, Comm'n Decision (Dec. 6, 2016), *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

[26] *Id.* (citing Case M.8124—Microsoft/LinkedIn, Comm'n Decision, ¶ 350 (Dec. 6, 2016), *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

certain markets, particularly where non-monetary transactions occur."[27] This does not mean, however, that competition law should subsume consumer data rights.

28. The maintenance of separate regimes is best for both the short- and long-term. Competition law is not the main avenue through which policymakers should protect consumer data or privacy. Competition law should only be used where the potential harm flowing from privacy protection measures is grounded in the actual or potential diminution of economic efficiency.[28] Confusing or conflating the scopes and roles of competition and consumer protection laws may dampen the mandates that they are each tasked with fulfilling, undermine their respective foundations, and unintendedly fail to address the consumer data and privacy concerns that emerge irrespective of the extent of competitive rivalry in the marketplace.

B. Need for Regulatory Cooperation

29. Consumer data rights and competition law should not be in practical or operational conflict. The goals of both regimes must be complementary or at least compatible, and the authorities must not seek to regulate behaviour in a manner that puts businesses offside of the other regulator.

30. Overregulation should be avoided as it can have a chilling effect on the market. To the extent that regulators take enforcement action, a lack of regulatory clarity can have this same effect. While the application of regulation in a given case may be sensible, enforcement decisions often have limited clarity on how other firms should apply decision to themselves. This concern is especially acute in innovation industries, such as e-commerce, social media and FinTech, which are growing in size and significance in the global economy.

31. Authorities' coordination of innovation demands will be particularly necessary in the context of remedies, where a remedy for a competition market failure, such as a case of data-sharing, may itself create a harm to consumers' privacy. There are scenarios where a firm that fails to protect consumer data experiences a loss of sales to their competitors, which signals that data protection quality can affect competition, for better or for worse.[29] Coordination of regulatory enforcement is key to ensure that innovation can continue to flourish without compromising either healthy competition or consumer data protection.

32. Where competition authorities and consumer protection and privacy agencies and commissions collaborate or advise one another, *Business at OECD* recommends frequent and open dialogue between regulators and experts across policy boundaries to consider and advance privacy and competition issues and goals. Regulators should invite (though not necessarily accept) non-binding opinions from other authorities whose assessments should be considered relevant to specific cases in ways that might change or at least enlighten regulator decision-making.[30]

33. Overall, while competition law regulations should not be blended into consumer data rights protection measures and vice versa, their enforcements efforts do not operate in isolation and must

---

[27] OECD Digital Zero-Price Markets Secretariat Note, *supra* note 16, ¶ 130.

[28] Ohlhausen & Okuliar, *supra* note 5, at 152.

[29] OECD, *Considering Non-Price Effects in Merger Control – Background Note by the Secretariat* ¶ 116 (June 6, 2018), *available at* http://one.oecd.org/document/DAF/COMP(2018)2/en/pdf.

[30] OECD Digital Zero-Price Markets Secretariat Note, *supra* note 16, ¶ 148.

therefore work in tandem. For example, competition remedies relating to privacy and data use and sharing should be drafted in such a way as to limit the potential for conflict with objectives under privacy and data protection laws.

C. Competition Law Enforcement – Theories of Harm re: Consumer Data

34. Privacy may be a relevant consideration in merger review if it is an aspect of competition upon which competitors compete. Mergers and other forms of data accumulation give rise to the concerns of non-consensual data sharing, as well as the fact that "compilations of even small and disconnected pieces of data" may together "reveal additional personal information about individuals, which [can] then be used for new purposes."[31] Industries where this can arise are banking, including credit lending, which store highly personal information that people consider private, rendering high levels of protection over consumer data a competitive advantage among banks. To the extent that the merging firms previously provided competitive discipline on each other in this area, one anti-competitive effect of the transaction may be a decrease in the quality of privacy protections.[32]

35. However, a decrease in privacy may not always be of concern to consumers. Recall the so-called "privacy paradox"; consumers' paradoxically believe that privacy is highly important, but are willing to provide personal information in order to access and optimize, at no or nominal cost, digital services such as search engines, online banking, and social networking and data apps. Indeed, research into revealed preferences (rather than stated preferences)[33] typically finds that consumers are willing to accept small discounts and purchase recommendations in exchange for personal data.[34] Although consumers indicate they are concerned about privacy, their marketplace behaviour demonstrates that their concerns "are not sufficient to slow the adoption of services that rely on the collection and use of their data."[35] As a result of the "privacy paradox," regulatory responses must consider both stated and revealed consumer preferences to ensure that beneficial uses of consumer data are not necessarily restricted.[36]

36. Privacy as a dimension of competition is a developing area. While there are examples of businesses capitalizing on privacy as a value niche,[37] "competition on [the basis of] privacy appears to still be observed in only a minority of competition cases."[38] This may in part be a product of consumers' difficulties in "evaluating privacy quality"[39] or consumers' decisions to trade privacy for the free use of products or services. Accordingly, competition authorities will need to consider both the existence

---

31 Ohlhausen & Okuliar, *supra* note 5, at 152.

32 OECD Digital Zero-Price Markets Secretariat Note, *supra* note 16, ¶ 39.

33 Stated preferences refer to what consumers state they prefer, and revealed preferences refer to the choices consumers make.

34 GAI Comment, *supra* note 17, at 14-15 (citing Dan Cvrecek, Marek Kumpost, Vashek Matyas & George Danezis, A Study on the Value of Location Privacy, Proceedings of the 5th ACM Workshop on Privacy in the Electronic Society (2006)).

35 *Id.* at 15.

36 *Id.*

37 For example, DuckDuckGo, an online search engine that does not retain search engine history, Ghostery, a security-protection add-on for internet browsers that helps users easily detect tools that advertisers use to track individuals across their Web explorations, and the many applications and social media platforms that include heightened privacy measures as part of their value propositions such as Backchat, Whisper, Ask.fm and SnapChat.

38 OECD Digital Zero-Price Markets Secretariat Note, *supra* note 16, ¶ 16.

39 *Id.*

and relevance of privacy and its competitive character (or lack thereof) on a case-by-case basis based on the evidence available in the context of the review of a specific merger or investigation.

37. Data, in conjunction with other inputs, can confer market power where such data—particularly B2B data—is an essential input for downstream competitors (a topic further discussed below) and may act as a barrier to entry into and expansion within a market. As an input, consumer data can help improve and better tailor products and services that online businesses generate.[40] As an example, a travel agency and metasearch engine may use data mining technology to analyze numerous queries run by consumers on its websites to predict price trends on airline flights for specific, customer-selected travel destinations. That service would not work without user search data. Another operator may offer a predicted price change timeline to prospective travelers, generating a recommendation on whether to buy now or to wait. These are just a couple of examples within one industry, travel price prediction, where consumer data is both an input and a commodity asset.[41]

38. The competition law "remedy" of democratizing data between businesses could have a ripple effect of reducing the competitiveness of industries overall. Enforced sharing of consumer data for general use may decrease incentives to collect and innovate using consumer data. This would reduce or eliminate the significant efficiencies generated by data use by businesses and with it, the benefits realized by consumers. If companies are forced to give information to other companies under competition law enforcement, private consumer data is at risk of experiencing security breaches and consumer protection would depreciate.[42] This is a lose-lose scenario for both businesses and individuals, while also contradicting the mandates of both competition law and consumer protection laws. Again, competition authorities must act only on evidence presented in specific circumstances and be careful in their approach to remedies.

39. Some suggest that consumer data could be considered an essential input and that withholding data from competitors is exclusionary conduct, and hence the essential facilities doctrine should apply. *Business at OCED* cautions, however, that consumer data is neither finite nor difficult to collect (i.e., firms may collect it themselves or acquire it from data brokers, data aggregators, and other suppliers that commonly supply telecom, media, entertainment and service providers). Moreover, the value of the data is derived by how the data is used not the data itself or the volume.[43]

40. Moreover, as with other circumstances where competitive harm is alleged to arise from the denial of access to essential facilities, competition authorities must execute their duties cautiously because there are trade-offs to remedies that affect businesses and consumers alike. Indeed, the cure may be worse than the illness, as sharing personal data itself raises consumer privacy concerns that put consumers at risk of having their personal information distributed to parties with which they did not originally consent to sharing such information. Similarly, there are also data security and

---

[40] *Id.* ¶ 122.

[41] Ohlhausen & Okuliar, supra note 5, at 131.

[42] Decisions of competition authorities often have to resolve issues of compliance with other laws. For example, the compliance with national data protection laws could be considered a justification for not sharing data. Privacy concerns may also be mitigated if consumers consent to the sharing of data. *See e.g.*, Mark Willis, French Competition Authority orders GDF Suez to give competitors access to customer data (Sept. 2014), *available at* https://www.twobirds.com/en/news/articles/2014/france/french-competition-authority-orders-gdf-suez-to-give-competitors-access-to-customer-data.

[43] The success of start-up firms lacking consumer data casts further doubt on suggestion that consumer data is an essential input (e.g., Google, Facebook, Twitter, Yelp and Pinterest).

protection concerns. This may be a particular issue in sectors such financial services, where requiring an established firm to provide a consumer data set to an emerging firm could result in data breaches.

41. Remedies may also increase costs for businesses required to provide such data, depleting their profit and potentially demanding other expensive changes to their cost structure and business plan, especially if such data sharing becomes an ongoing, integrated, or mandatory obligation or order.

42. Another risk of overregulation is the cannibalization of many of the positive outcomes of consumer data collection (e.g., services provided to consumers as a result of data collection). While data collection can in certain circumstances lead to bias, it can also be used to reduce bias. Extensive data collection, which may involve private or sensitive data on race, ethnicity, gender and other attributes may assist in the detection and remedy of bias on discrimination within online business platforms and services. If companies become averse to collecting personal information for the purposes of avoiding stringent competition regulations that may mandate access to such data, the benefits that consumer data collection afford both companies and individuals fade.

43. Efficiencies and total consumer welfare to the extent applicable should be considered in assessing alleged harm. In the absence of conclusive evidence of the negative effects on competition associated with the aggregation of personal data, and in the presence of real benefits of innovation in the digital economy offering consumers access to new markets, increased choice of goods and services, and lower search costs, *Business at OECD* recommends that "the risk of over-enforcement should be weighed particularly carefully by [competition] authorities tempted to intervene."[44]

V. Conclusion

44. As increased attention is directed towards the growing collection and use of consumer data, *Business at OECD* recommends that measures aimed at addressing concerns arising from this phenomenon be carefully tailored to avoid chilling innovation and investment. *Business at OECD* supports delineating the scope of competition law alongside the evolving sphere of consumer data rights, including privacy, to ensure that regulators and policymakers work within their parameters and avoid inefficient forms of enforcement, including ex ante, or other rigid forms, of regulation. This approach will minimize the negative consequences associated with overregulation, and will allow the positive outcomes of data-based developments to flourish.

45. *Business at OECD* therefore recommends that continued responsibility for enforcing market failures relating to consumer data remain with consumer protection agencies, including those governing privacy, and that competition enforcement remain focused on failures relating to market competition. These agencies and competition authorities should coordinate their advocacy and enforcement activities in a manner that creates as much certainty and predictability as possible. By avoiding or at least minimizing regulatory overlap, these agencies will reduce unnecessary uncertainty about compliance for consumers and businesses alike, permitting both to benefit from the results of enhanced business efficiency and innovation.

---

[44] *Business at OECD* Personalised Pricing Paper, *supra* note 1, ¶ 19.