Organisation for Economic Co-operation and Development

DAF/COMP/WD(2020)39

Unclassified

English - Or. English

12 June 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Consumer data rights and competition – Note by the United States

12 June 2020

This document reproduces a written contribution from the United States submitted for Item 3 of the 133rd OECD Competition Committee meeting on 10-16 June 2020.

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

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

JT03462940

United States

1. Introduction

1. In the United States, a number of federal and state statutes address consumer data rights and related concerns. The Federal Trade Commission (FTC) and the United States Department of Justice (DOJ) are responsible for enforcing laws relating to the privacy and security of consumer data and federal competition laws.[1]

2. On the consumer data rights side, the FTC has brought hundreds of cases and obtained billions in penalties to protect the privacy and security of consumer data,[2] enforcing the FTC Act's general prohibition of *"unfair or deceptive acts or practices in or affecting commerce"*.[3] The FTC also enforces domain specific statutes such as the Children's Online Privacy Protection Act of 1998 (COPPA),[4] which restricts collection and use of personal information pertaining to children under the age of thirteen, the Fair Credit Reporting Act (FCRA),[5] which protects information collected by consumer reporting agencies, and the Financial Services Modernization Act of 1996 (Gramm-Leach-Bliley Act or GLB),[6] which regulates the use and dissemination of consumers' "non-public personal information" by "financial institutions," broadly defined. The FTC also enforces federal competition law.

3. The DOJ's Civil Division, Consumer Protection Branch, brings both criminal and civil enforcement actions to protect consumers' health, safety, economic security, and identity integrity. This work often implicates consumer data and privacy rights. The Consumer Protection Branch's civil authorities include jurisdiction over actions referred by the FTC seeking civil penalties under the FTC Act.[7] It also has broad criminal authorities to carry out its mission. The DOJ's Antitrust Division has separate authority to enforce the federal competition laws.

---

[1] Additional, sector-specific privacy and data security enforcement is shared with, e.g., the US Department of Health and Human Services, which enforces certain protections regarding electronic health information. *See, e.g.*, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, as amended (codified at 42 USC §§ 1320d et seq.). Implementing regulations, the HIPAA privacy, security, and enforcement rules, are at 45 CFR Parts 160 and 164.

[2] *See, e.g.*, Fed. Trade Comm'n, Privacy & Data Security Update: https://www.ftc.gov/reports/privacy-data-security-update-2019 (noting, through calendar year 2019, more than 130 spam and spyware cases and 80 general privacy lawsuits, including a $5 billion settlement with Facebook, id. at 2; more than 75 data security cases, including a $375 million settlement with Equifax, id. at 5; more than 100 Fair Credit Reporting Act cases, id. at 7; close to 30 cases under the Children's Online Privacy Protection Act (COPPA)since 2000, id. at 8; about 35 cases under the Gramm-Leach-Bliley Act on financial institution privacy notices, id. at 7; and almost 150 cases enforcing do-not-call provisions, id. at 10.

[3] 15 U.S.C. § 45(a)(1).

[4] 15 U.S.C. §§ 6501-6506.

[5] 15 U.S.C. §§ 1681-1681x.

[6] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.)

[7] 15 U.S.C. 56(a)(1).

4. This note articulates some of the potential interfaces of consumer data rights with competition, which may be of import to policy makers.[8]

2. Overview

5. Digital markets are integral to our economy, and use of consumer data is ubiquitous.[9] Data—broadly construed—now comprise both inputs and outputs for many goods and services across diverse sectors of the economy. Products simultaneously generate and capture digital trails, and the amount of information about individuals that is collected, stored, and analyzed with increasingly sophisticated tools is vast, and increasing.[10]

- Such data are diverse in nature, format, and application, and have significant economic value for both firms and consumers; for example, research using various methodologies suggests that high levels of consumer surplus—the difference between consumers' willingness to pay to access a service and the amount they actually pay—are associated with online services that have nominal prices of zero.[11]
- This dynamic is especially apparent in online advertising. In May 2019, the DOJ's Antitrust Division held a public workshop to explore industry dynamics in media advertising, with a focus of the rise in importance of digital advertising. During the workshop, panelists described behavioral advertising—the type of advertising that targets consumers based on data about their background and preferences—as a lucrative business and a prominent business model for many online platforms that provide users with digital services or content. Some panelists also lamented a lack of competitive alternatives for consumers who sought more privacy-friendly providers of online content.

[8] Consumer data rights policy, regulation, and enforcement issues relate to decades of work at the Organization for Economic Cooperation and Development (OECD), dating back at least to the 1980 OECD guidelines on the protection of privacy and transborder flows of personal data, which followed on the 1973 fair information practices principles developed in the United States. The United States has long supported this work and recognized its importance, participating actively in the Committee for Digital Economic Policy's working parties on privacy and security, and in the Committee on Consumer Policy.

[9] We recognize that concepts—and regulatory definitions—of "consumer data," "personal information," or "personally identifiable information" vary, and our default construction of them, throughout this document, is broad.

[10] For example, a 2014 report on data brokers by the Federal Trade Commission observes that "one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements," and that another broker "has 3000 data segments for nearly every US consumer." Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability, iv (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. And data collection, analysis, and transmission have continued apace since the publication of that report.

[11] For example, Brynjolfsson, Collis, and Eggers use a combination of different survey methodologies to show that high levels of consumer surplus are associated with free online content. Erik Brynjolfsson, Avinash Collis & Felix Eggers, *Using Massive Online Choice Experiments to Measure Changes in Well-being*, 15 PROC. NAT'L ACAD. SCI.7520 (2019). *See also*, Leonard Nakamura, et al., "Free" Internet Content: Web 1.0, Web 2.0, and the Sources of Economic Growth, Fed. Reserve Bank of Philadelphia Working Papers, WP 18-17 (2018), https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-17.pdf. Nakamura, et al. (2018) (analyzing contribution of "free" content to domestic production).

6. Legal and regulatory regimes create or recognize certain rights, prerogatives, or entitlements pertaining to data, as well as positive and negative obligations regarding data collection, use, and transmission. Such rights and obligations may relate, for example, to data security, or to the disclosure of certain data-related practices.

7. Rights and obligations relating to consumer data may affect competition. For example:

- Some data rights and obligations may enhance competition, for instance, by reducing information asymmetries or by deterring exclusionary conduct.[12]
- Other rights and obligations may impair competition, for instance, by entrenching market power.[13] For example, Campbell, Goldfarb, and Tucker use a microeconomic model to argue that, due to economies of scale in data collection and utilization, certain privacy regulations, though imposing costs on all firms, may have a particularly adverse effect on smaller and new firms, especially in cases where firms offer zero-priced consumer services.[14]
- While not definitive, empirical evidence suggests that data rights may affect markets and competition in a variety of ways, including:

2.1. Financial markets:

8. On the firm side, Hertzberg, et al.,[15] and Doblas-Madrid and Minetti[16] study the effects of information sharing on firms in credit markets. Doblas-Madrid and Minetti use contract-level data from a US credit bureau in the equipment financing industry to examine the impact of lenders' access to information about borrowing firms' repayment performance on the credit performance of firms. They find that access to such information in their sample can reduce contract delinquencies and defaults, without loosening lending standards. Hertzberg, et al., using data from the Argentine public credit registry, further suggest that information sharing among lenders about borrowing firms' repayment performance may reduce the incidence of delinquencies and defaults, but that lenders may also reduce credit to a firm in anticipation of other lenders' reaction to negative news about the firm.

[12] *See, e.g.*, Fed. Trade Comm'n, Hearings: Competition and Consumer Protection in the 21st Century, Privacy, Big Data, and Competition (Nov. 7, 2018), M. Baye, Transcript at 14; J. Baker, Transcript at 15-20, https://www.ftc.gov/system/files/documents/public_events/1418633/ftc_hearings_session_6_transcript_day_2_11-7-18_1.pdf. [hereinafter FTC Hearings, Privacy, Big Data, and Competition]

[13] U.K. Digital Competition Expert Panel, Unlocking Digital Competition: Report of the Digital Competition Expert Panel, 1.71-1.79 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf; FTC Hearings, Privacy, Big Data, and Competition (Nov. 7, 2018), A. Okuliar, Transcript at 29-31; M. Ohlhausen (Nov. 8, 2018), Transcript at 84-85.

[14] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47 (2015).

[15] Andrew Hertzberg, et al., *Public Information and Coordination: Evidence from a Credit Registry Expansion*, 66 J. FIN. 379 (2011).

[16] Antonio Doblas-Madrid & Raoul Minetti, *Sharing Information in the Credit Market: Contract-level Evidence from US Firms*, 109 J. Fin. Econ. 198 (2013).

9. On the consumer side, Kim and Wagman[17] study the impact of opt-in and opt-out defaults that determine whether lenders can share information about borrowing consumers on certain aspects of mortgage markets. Using variation in the adoption of local financial-privacy ordinances in five California Bay Area counties, they suggest that more stringent restrictions on the sharing of consumer financial information[18] may reduce price competition. They argue that such a reduction may take place due to sellers' inability to offset potential downstream costs from loan defaults with revenues from monetizing information obtained in the application process, and, consequently, lenders' incentives to screen applications from consumers may weaken, contributing to higher rates of loan defaults.

2.2. Healthcare:

10. Miller and Tucker, using variations across state medical privacy laws, suggest that certain state privacy regulations (adopted above minimum federal requirements) that restrict a hospital's release of patient information diminished the adoption of electronic medical records (E.M.R.s), reducing market efficiency in turn. First, they demonstrated local network effects in hospitals' adoption of E.M.R. systems, and found that certain state requirements for patient consent tended to suppress those network effects and, consequently, the rate of E.M.R. adoption.[19] Second, they found that the reduction in efficiency could have a significant impact on certain healthcare outcomes.[20] Miller and Tucker assert that the interaction between data regulations, innovation, and information flow may be complex. For instance, they argue that state-specific regulation may impose costs by increasing regulatory complexity and uncertainty,[21] and that explicit privacy protection could promote the use of information technology by reassuring potential adopters—and their consumers—that sensitive information will be protected.[22]

---

[17] Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, 46 RAND J. Econ. 1 (2015).

[18] Specifically, in 2002, three out of five counties in the San Francisco-Oakland-Fremont, California Metropolitan Statistical Area adopted local ordinances that were more protective than previous practices, in that the new ordinances required financial institutions to seek written waivers from consumers before sharing information about those consumers with either affiliates or non-affiliates.

[19] Amalia R. Miller & Catherine Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records*, 55 MGT. SCI. 1077 (2009). Because both regulation and substantial federal subsidies under, e.g., the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009), have prompted nearly universal adoption of electronic health records systems (EHRs) by US hospitals, there is a question about whether the magnitude of the demonstrated network effect still applies. This was, however, a well-designed study with ongoing relevance to the investigation of, e.g., network effects, spillover, unanticipated, or even perverse effects that may be associated with, or caused by, privacy regulations.

[20] Amalia R. Miller & Catherine E. Tucker, *Can Health Care Information Technology Save Babies?*, 119 J. POL. ECON. 289 (2011).

[21] *See* Miller & Tucker (2009), *supra* note 19, and Miller & Tucker (2011), *supra* note 20. *See also*, text accompanying note 24 below, regarding Adjerid, et al. and Health Information Exchange adoption. For a discussion of complex regulatory impediments, among others, to the adoption of health information technology and the flow of healthcare information, *see., e.g.*, Daniel J. Gilman & James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking The Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279 (2010).

[22] Recent OECD works endorse the notion of fostering consumer trust. *See, e.g.*, the OECD "Going Digital" project: "Trust in digital environments is essential; without it, an important source of economic and social progress will be

11. One example of the aforementioned dynamic is from Health Information Exchanges (HIEs). HIEs are information-technology solutions that facilitate the sharing of patients' electronic medical records among healthcare entities, with the aim of improving quality of care.[23] Their adoption, however, may be hindered by both privacy concerns on the consumer side and by privacy laws that restrict the disclosure of health records on the healthcare provider side. Adjerid, et al. compare the formation of HIEs in states with laws that limit information disclosure with states that do not have such laws.[24] They suggest that in their sample, certain relatively strong privacy policies tend to suppress HIE adoption, but that the combination of adoption subsidies and some stronger privacy protections is associated with greater HIE adoption than subsidies, stronger privacy protections, or weaker privacy protections alone. They argue that regulators may find room to balance meaningful privacy protections with incentives for the adoption of new healthcare technologies.

12. Miller and Tucker also identify three approaches taken by states to protect patients' genetic privacy with data rights: requiring informed consent; restricting discriminatory usage by employers, healthcare providers or insurance companies; and limited re-disclosure without consent.[25] Their empirical findings suggest that, in their sample, the re-disclosure approach increases the diffusion of genetic testing, in contrast to the informed consent approach, which may deter it.

2.3. Online advertising:

13. In "Privacy Regulation and Online Advertising," Goldfarb and Tucker examine the effects of the implementation of the 2002 European Union (EU) ePrivacy Directive, which limited the ability of advertising networks to collect user data in order to target ads, and conclude that, after it took effect, advertising effectiveness in the EU in their sample decreased significantly.[26] Their study uses the responses of 3.3 million survey-takers who had been randomly exposed to 9,596 online banner ad campaigns. For each of the campaigns, their dataset contains a treatment group exposed to the ads and a control group exposed to a public service ad. To measure ad effectiveness, they use a short survey conducted with both groups of users about their purchase intent towards an advertised product. They find that, following the ePrivacy Directive, banner ads in their sample experienced a reduction in effectiveness of over 65%, with no similar changes in

left unexploited" (https://goingdigital.oecd.org/en/dimension/trust/). *See also* the OECD Council Recommendation on Digital Security Risk Management for Economic and Social ("calls on the highest level of leadership in government and in public and private organisations to adopt a digital security risk management approach to build trust and take advantage of the open digital environment for economic and social prosperity…"), http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf. *Cf. also* "Trust in Peer Platform Markets/Consumer Survey Findings," https://www.oecd-ilibrary.org/science-and-technology/trust-in-peer-platform-markets_1a893b58-en

[23] Centrally, these are agreements about the sharing of information among providers, although the implementation of such agreements may entail technical and standards endeavors as well.

[24] Idris Adjerid, et al., *Choice Architecture, Framing, and Cascaded Privacy Choices*, 65 MGMT. SCI. 1949 (2019). In all cases, such information sharing may be subject to federal and state laws. The distinction studied, however, turns on the question of whether the individual states impose additional express restrictions on the sharing of such information between health care providers.

[25] Amalia R. Miller & Catherine Tucker, *Privacy Protection, Personalized Medicine, and Genetic Testing*, 64 MGT. SCI. 4471 (2018).

[26] Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGT. SCI. 57 (2011).

non-European countries during a similar timeframe. They assert that it is possible that data rights can have a detrimental effect on the efficiency of online advertising.

14. A recent study by Johnson, Shriver, and Du[27] examines the AdChoices Program, an ad industry program (begun in the US) that enables consumers to opt out of behavioral advertising via a dedicated website that can be reached by clicking an AdChoices icon overlaid on internet ads.[28] Based on a data sample from an ad exchange, they suggest that US users who opt out fetch 52% less ad revenue on the exchange than users who allow behavioral targeting, who are presented with comparable ads. They assert that these costs are borne by publishers and by the exchange, and observe similar results in their sample for the EU and Canada. Other researchers have questioned the extent to which publishers benefit from targeted advertising; for example, a study by Marotta, et al. suggests that publishers derive a 4% increase in revenue from engaging in targeted advertising.[29] While the effects may be difficult to measure,[30] and may vary across publishers, the impact of potential or actual losses in advertising revenue may merit consideration of potential downstream effects on competition and consumer surplus.

2.4. New firms and investment:

15. The connection between data rights and new firm formation is highlighted by recent research on the impact of the EU's 2018 General Data Protection Regulation (GDPR) on investment in new technology ventures. Jia, Jin, and Wagman analyze venture investment data from two databases that track global venture investments and find evidence suggesting dramatic drops in investments in newer, 0-6 year old EU technology ventures after GDPR.[31] Their findings hold more strongly for consumer-facing ventures that are in their initial development stages. Although further, and broader, study of the impact of GDPR is warranted, the magnitude of early findings regarding venture capital investment suggests the potential for substantial effects, at least for certain data rights. It will be important to see what such effects look like over time, as businesses and regulators adjust to the effects of the regulation.

16. Results from the above studies, among others, illustrate some of the trade-offs that may be implicated by data rights, and may suggest a need to account for, and balance, specific and continually evolving trade-offs in policy making.

17. 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.

---

[27] Garrett Johnson, Scott Shriver & Shaoyin Du, *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, 39 MRK. SCI. 33 (2020).

[28] *Id.*

[29] Veronica Marotta, et al., *Online Tracking and Publishers' Revenues: An Empirical Analysis*, Workshop of Information Systems Economics (WISE) (2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

[30] Regarding some of the difficulties associated with measuring the causal effects of digital advertising, see, e.g., Brett Gordon, et al., *A Comparison of Approaches to Advertising Measurement: Evidence from Big Field Experiments at Facebook*, 38 MARKETING SCI. 193 (2019).

[31] Jian Jia, et al., *The Short-Run Effects of GDPR on Technology Venture Investment*, NBER Working Paper No. 25248 (2018; updated 2019). https://www.nber.org/papers/w25248

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.[32]

3. Economic modeling at the interface of data and competition

18. Data issues may play a role in merger review: An increasing number of mergers in the digital sector involve data.[33] While merger review is concerned with competitive effects, the analysis of these effects may, in individual cases, involve examination of data or data rights held by the merging parties. The modeling of mergers and competition under different data regimes points to a number of areas of interest, including:

- Competition and mergers: the potential impact of data on a merger tends to be industry and case specific. In "The Economics of Privacy," Acquisti, Taylor and Wagman provide a synthesis of the literature.[34]

19. Salient theoretical papers include the following:

- Cooper, et al., use a microeconomic model to study spatial price discrimination and contrast, in particular, three-to-two mergers when firms do and do not have access to detailed consumer information.[35] The authors' model suggests that access to detailed consumer information and the ability to set prices that condition on that information may cause a merger to have less of an anti-competitive price effect than if firms lacked this information or the ability to charge anything but uniform prices.
- Kim, et al., construct a microeconomic model to examine merger incentives and consumer welfare when firms have access to consumer data, and contrast it with the case where there is relatively little available data.[36] Their analysis suggests that access to consumer data in a market (e.g., for purposes of marketing, price discrimination, and market segmentation) can lead to lesser reductions in consumer surplus from mergers, provided such mergers are not mergers to monopoly.
- Cornière and Taylor construct a microeconomic model that suggests that whether privacy rights are pro- or anti-competitive depends upon whether the relationship

[32] Recognition of such policy tradeoffs is found in, e.g., FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report; EXECUTIVE OFFICE OF THE PRESIDENT PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf; OECD, Directorate for Fin. and Enterprise Affs. Comp. Comm., Implications of E-Commerce for Competition Policy—Note by the United States (Jun. 6, 2018), https://one.oecd.org/document/DAF/COMP/WD(2018)48/en/pdf.

[33] *See, e.g.*, Elena Argentesi, et al., Ex Post Assessment of Merger Policy in Digital Markets, Lear, Report Prepared for U.K. Competition and Markets Authority (2019), https://www.learlab.com/wp-content/uploads/2019/06/CMA_past_digital_mergers_GOV.UK_version-1.pdf.

[34] Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016).

[35] James C. Cooper, Luke M. Froeb, Daniel P O'Brien & Steven Tschantz, *Does Price Discrimination Intensify Competition? Implications for Antitrust*, 72 ANTITRUST L.J. 327 (2004-2005).

[36] Jin-Hyuk Kim, Liad Wagman & Abraham L. Wickelgren, *The Impact of Access to Consumer Data on the Competitive Effects of Horizontal Mergers and Exclusive Dealing*, 28 J. ECON. & MGMT. STRATEGY 373 (2019).

between consumer utility and firm revenue is that of complements or substitutes, respectively, although when the relationship is one of complements, it could also lead to higher levels of market concentration.[37]

4. Antitrust analysis at the interface of data and competition

20. In appropriate cases, access to data may be an important precondition for competitive entry or for certain kinds of innovation, and antitrust enforcers can and should consider such effects when they are likely in individual cases.[38] Examples of such cases include the following.

- In *United States v. Thomson Corp.,* [39] DOJ required the divestiture of three financial data sets that were used by investment managers, investment bankers, traders, corporate managers, and other institutional customers in making investment decisions and providing advice to their firms and clients. The data in question were investment fundamentals data, earnings estimates data, and aftermarket research reports. DOJ concluded that the merger of Thompson Corp. and Reuters would have eliminated competition between the two companies and led to higher prices and reduced innovation for fundamentals data, earnings estimates data, and aftermarket research reports. The settlement required the merging parties to sell copies of specified data sets and required licensing of related intellectual property.
- In *United States v. Google Inc.*, [40] Google purchased ITA Software, Inc. (ITA), the leading vendor of software to search for, price, and display results for airline travel queries. DOJ determined that the proposed transaction could harm competition for airfare comparison and booking websites and diminish effective competition among websites using ITA's software to compete against any airfare website that Google might introduce. Two competitive concerns relevant to this paper were that Google, through the purchase of ITA would (1) obtain access to competitors' proprietary data in order to compete with those competitors and (2) deny competitors access to ITA's pricing and shopping software. The final judgement therefore required the merging parties to establish an internal firewall to prevent the misappropriation of competitively sensitive data and to license ITA's software to airfare websites on commercially reasonable terms. Google also was required to continue to fund research and development of that software at least at levels similar to what ITA had invested in prior years and to further develop and offer ITA's next software.
- In *United States v. CVS*,[41] DOJ required the merging parties to divest Aetna's individual Medicare Part D prescription drug plan business to resolve the

[37] Alexandre de Corniere & Greg Taylor, *Data and Competition: A General Framework with Applications to Mergers, Market Structure, and Privacy Policy*, CEPR Discussion Paper No. DP14446 (February 2020) https://ssrn.com/abstract=3547379.

[38] A transaction could also affect non-price attributes of competition, such as consumer privacy or data security. *See, e.g.*, statement of Fed. Trade Comm'n Concerning Google/DoubleClick, FTC File No. 071-0170, 2-3 (Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

[39] *See, e.g.*, United States v. Thomson Corp., 2008 Trade Cas. (CCH) P76,190 (D. D.C. 2008).); United States v. Deutsche Telekom AG, 2020 U.S. Dist. LEXIS 6509 (D. D.C. 2020).

[40] United States v. Google Inc., 2011-2 Trade Cas. (CCH) P77,617 (D. D.C. 2011).

[41] United States v. CVS Health Corp., 407 F. Supp. 3d 45, 2019 U.S. Dist. LEXIS 150645, 2019-2 Trade Cas. (CCH)

competitive concerns of higher prices for Medicare beneficiaries and taxpayers and lower quality service caused by the elimination of head-to-head competition between CVS and Aetna. Because continuity is important to retaining customers, DOJ required that this divestiture include historical data related to the divested plans and broker contracts. Both the retail pharmacy rates for various drugs and the broker commissions frequently are negotiated on an annual basis, and significant changes to either can cause disruption for consumers. By requiring the divestiture to include historical data, DOJ provided the divestiture buyer with the opportunity to replicate the prior cost structure and avoid price increases.

- In *CoreLogic, Inc.*,[42] data were both a product and a divestiture asset, and the scope of a historical database in particular was seen as a barrier to entry for would-be competitors. The FTC alleged that the proposed acquisition would substantially lessen competition in the market for national real estate assessor and recorder bulk data by merging two of only three firms licensing such data, increasing the risk of anticompetitive coordination between the two remaining market participants and the risk that CoreLogic would unilaterally exercise market power and raise prices. The data in question comprised public information about individual real estate properties, including descriptive information, such as square footage and the number of bedrooms, and financial data, such as purchase price, mortgage terms, and lien details. The settlement required that CoreLogic license bulk data, as well as several ancillary data sets, to a third-party entrant, to enable it to compete.
- In Verisk/EagleView,[43] the FTC challenged the proposed merger based on innovation effects related to data quality and coverage, alleging that the merger would likely reduce competition and result in a virtual monopoly in the US market for rooftop aerial measurement products used by the insurance industry to assess property claims. Data were regarded as necessary inputs into a relevant product market, where the acquirer's position in an adjacent market provided it with a unique opportunity to overcome data-related entry barriers. Although the data in question were not paradigmatic of things ordinarily considered personal information, the aerial image libraries at issue were images of consumer homes (specifically, the roofs and surrounding property), which were combined with insurance information.

5. Navigating the interface of consumer data rights and competition

21. Assigning or establishing consumer data rights can have complex competitive effects. Such provisions may create presumptions or defaults about who controls, owns, or has the right to exclude others from using valuable information. This assignment to one party or another may clarify the terms under which marketplace actors can transact and transfer data, potentially reducing ambiguity or other uncertainty about locus or scope of data rights. At the same time, as observed in the research cited above, the creation, assignment and/or specific implementation of data rights can have complex effects.

P80,908, 2019 WL 4194925.

[42] CoreLogic, Inc., FTC Docket No. C-4458 (FTC 2014), https://www.ftc.gov/enforcement/cases-proceedings/131-0199/corelogic-inc-matter (admin. complaint).

[43] Verisk/EagleView, FTC Docket No.9363 (FTC 2014), https://www.ftc.gov/enforcement/cases-proceedings/141-0085/veriskeagleview-matter (admin. complaint).

22. The US government's regulation of consumer data rights has sought to address these complex effects, fostering competition and innovation while providing effective protection for consumers, looking to prevention and redress of harms as the primary purpose of the regulatory and enforcement action.[44] The FTC and DOJ's enforcement actions involving privacy and data security have accordingly addressed harms such as financial injury, physical harm, reputational injury, unwarranted intrusions into people's intimate lives, and unwanted commercial intrusions such as telemarketing, spam, and debt collection harassment.[45] Certain areas of US consumer protection law pertinent to privacy and data security also expressly link violations to the distortion of market behavior or consumer harm. For example, under the FTC Act's general prohibition of *"unfair or deceptive acts in or affecting commerce"*,[46] unfair acts or practices must be *"likely to cause substantial injury to consumers … not outweighed by countervailing benefits to consumers or to competition"*;[47] and a false advertisement is one where *"the basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service . . . [and] consumer injury is likely, because consumers are likely to have chosen differently, but for the deception."*[48]

23. Many US cases have focused on net harmful commercial data practices where consumers cannot effectively bargain to avoid those harms. Examples include, but are not limited to, spam, revenge porn, fraud, and deception.

- To highlight a case involving one of the largest collectors of user data, Facebook agreed in 2012 to an FTC order to settle allegations that its practice of sharing "Affected Friends' data" with third-party developers of apps was deceptive.[49] In

[44] Cf. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015), which includes a "preventing harm" principle: "acknowledging the risk that harm may result from … misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information."

[45] *See* the FTC Staff Comment to the NTIA: Developing the Administration's Approach to Consumer Privacy (2018), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf; *see also, e.g.*, recent actions involving DOJ's Consumer Protection Branch, including: *United States v. Boling, et al.*, No. 19-cr-0524 (W.D.T.X. 2019) (indicting multiple defendants for using stolen personal data to compromise health-benefit and banking systems to defraud thousands of US service members and veterans), https://www.justice.gov/opa/pr/five-fraudsters-indicted-million-dollar-scheme-targeting-thousands-us-servicemembers-and; *United States v. Musical.ly, et al.* [now TikTok], 19-cv-1439 (C.D. Ca. 2019) (settling alleged violations of the FTC's COPPA Rule); *United States v. Aegerion*, No. 17-cr-10289 (D. Mass. 2017) (resolving company's criminal liability for obtaining patients' health data without authorization for commercial gain in violation of the Health Insurance Portability and Accountability Act), https://www.justice.gov/opa/pr/drug-maker-aegerion-agrees-plead-guilty-will-pay-more-35-million-resolve-criminal-charges-and; *United States v. Dish Network LLC*, No. 09-cv-3073 (C.D. Ill. 2017) (securing $280 million in civil penalties for violations of the FTC's Telemarketing Sales Rule), *aff'd in part* (7th Cir. 2020), https://www.justice.gov/opa/pr/justice-department-ftc-wins-largest-ever-telemarketing-penalty-against-dish-network.

[46] 15 U.S.C. 45(n).

[47] 15 U.S.C. 55(a)(1).

[48] FTC Statement on Deception, 103 F.T.C. 174, 175 (1984) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110 (1984)) ("Deception Policy Statement").

[49] United States v. Facebook, Inc., Civ. Action No. 19-2184, 3 (D.D.C. 2020) (complaint for civil penalties, injunction, and other relief). The complaint alleges that as early as 2010, every Facebook user who installed a third-party app agreed by default to Facebook sharing with the third-party app developer information about both the

2019, the FTC investigated Facebook again, for violating both the 2012 order and the FTC Act. The FTC and DOJ alleged that Facebook misrepresented consumers' ability to control their data by sharing it with app developers in contravention of explicit privacy promises. The FTC and DOJ also alleged that Facebook misrepresented that it was collecting information for security purposes, when it actually used that information for advertising purposes.[50] The FTC and DOJ settled this second case against Facebook with a $5 billion penalty, in addition to substantial behavioral remedies.[51]

- To highlight a case involving data security, in *Wyndham*,[52] detection of demonstrable consumer harm—large clusters of fraudulent credit card usage—led to the investigation of the firm's data security practices, and of its representations about those practices. Published material from the FTC's Bureau of Economics outlines the assessment of consumer harm, which included both direct financial losses and time spent to remedy those losses and guard against future ones.[53] FTC staff also took into account the estimated baseline rate of identity theft, conditional on a consumer being subject to a breach. And, because the Section 5 violation was predicated on the firm's deceptive statements, staff also estimated the price premium that consumers paid due to those deceptive statements, multiplied by an estimate of the number of consumers affected.[54]

24. In other instances, consumers may be able to bargain more effectively for privacy or data security. Like other features that make a service appealing to particular consumers, privacy can be an important qualitative, or non-price, dimension of competition. Firms that service such consumers, for example, may be spurred, through robust competition, to offer better privacy and/or data security protections. Without competition, a dominant firm may be able to reduce the quality of its goods or services—for example, consumers' preferred privacy or data security protections—without losing a significant number of users. At the same time, it remains to be seen how consumer behavior in the digital marketplace relates to expressed preferences for privacy. Although many consumers report that they care about privacy, consumers often relinquish their information for relatively small incentives—a disparity that is sometimes called the "privacy paradox."[55] The reasons for this apparent

installer and the installer's Facebook Friends ("Affected Friends"), even if those Affected Friends had not themselves installed the app. In light of that conduct, Facebook was alleged to have misrepresented the extent to which consumers could control the privacy of information that Facebook had about them, the steps that consumers needed to take to implement such controls, and the extent to which Facebook made user information accessible to third parties. *Id.*

[50] *Id.* at 4-6.

[51] *Id.* at 4-6.

[52] FTC v. Wyndham Worldwide Corp. et al., Civil No. 13-1887 (D.N.J. Apr. 7, 2014) (opinion denying defendant's motion to dismiss); 799 F.3d 236 (3d Cir. 2015).

[53] Dan Hanner, Ginger Zhe Jin, Marc Luppino & Ted Rosenbaum, *Economics at the FTC: Horizontal Mergers and Data Security*, 49 REV. INDUS. ORG. 613 (2016) (section on estimating harm from data breaches with application to *Wyndham* at 627 – 630).

[54] *Id.* Harm-based penalties do not preclude firms from engaging in conduct that, while causing some degree of harm, is beneficial on net. A regime based on addressing completed or likely harm is akin to protecting consumer data with a liability rule.

[55] Assistant Attorney General Makan Delrahim, *Blind[ing] Me With Science*, *Antitrust, Data, and Digital Markets*, Remarks at Harvard Law School & Competition Policy International Conference on "Challenges to Antitrust in a Changing Economy," Cambridge, MA (Nov. 8, 2019).

paradox, and its implication for privacy regulation and enforcement, are the subject of considerable academic attention and debate.[56]

25. In assessing the effectiveness of data rights and the data policies of firms and marketers, regulators and enforcers should also consider the externalities associated with the sharing of information by users who may be less privacy sensitive. For example, Acemoglu, et al., construct a microeconomic model of a data market where there are externalities associated with information shared by users about themselves, in that doing so may reveal information about others.[57] They demonstrate that due to such externalities, the value of an individual user's information (e.g., about the user's preferences) is low—because, to a degree, the user's information can be inferred from data shared by other users—and competition may not mitigate this effect.[58]

26. Additionally, it may be possible to identify areas where consumers uniformly benefit from data rights but the interface with competition is negligible (e.g., permitting users to delete their profiles if they wish to do so or to opt out of new data practices, in the event of a merger that is permissible on competition grounds).[59] For example, a letter from the Director of the FTC's Bureau of Consumer Protection notes that, independent of the permissibility of the acquisition itself, *"WhatsApp has made a number of promises about the limited nature of the data it collects, maintains, and shares with third parties—promises that exceed the protections currently promised to Facebook users. We want to make clear that WhatsApp must continue to honor these promises to consumers. Further, if the acquisition is completed and WhatsApp fails to honor these promises, both companies could be in violation of Section 5 of the Federal Trade Commission (FTC) Act and, potentially, the FTC's order against Facebook."*[60]

6. Advocacy

27. Given the potential for consumer data rights to have substantial competition effects, competition advocacy has an important role to play in data policy.

- Such advocacy is important given the ubiquity of both data and consumer data issues across the economy, the potentially significant interaction between consumer data rights (and related regulations) with competition and innovation, the importance of disseminating lessons from competition matters across diverse regulators, the potential stickiness or durability of inadvertent competitive harms produced by laws and regulations, and the limited legal authority antitrust agencies

[56] *See, e.g.*, Daniel J. Solove, *The Myth of the Privacy Paradox* (February 11, 2020). 89 GEO. WASH. L. REV. (2021) (forthcoming); GWU Legal Studies Research Paper No. 2020-10, https://ssrn.com/abstract=3536265.

[57] Daron Acemoglu, et. al, *Too Much Data: Prices and Inefficiencies in Data Markets*, NBER Working Paper No. 26296 (Sept. 2019), https://www.nber.org/papers/w26296.

[58] *Id.*

[59] *See, e.g.*, Letter From Jessica L. Rich, Director of the Fed. Trade Comm'n Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc. (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf; *see also*, OECD, Directorate for Fin. and Enterprise Affs. Comp. Comm., Implications of E-Commerce for Competition Policy—Note by the United States (Jun. 6, 2018), https://one.oecd.org/document/DAF/COMP/WD(2018)48/en/pdf.

[60] Letter from Jessica L. Rich, *supra* note 58, at 1.

may have over policy and enforcement decision-making that can significantly impact competition.[61]

- The FTC Act, which establishes and authorizes the FTC, also gives the FTC a research, education, and policy mission. In particular, the FTC is to investigate and report on market developments in the public interest and make legislative recommendations based on its findings.[62] For example, FTC staff have advised sectoral regulators on competitive implications, including possible benefits and harms, of interoperability policies,[63] and both competition and consumer privacy issues implicated in national "information blocking" and certification regulations for health information and health IT.[64] FTC staff have also commented about the balancing of consumers' interests in privacy, competition, and innovation in a national telecommunications policy (FTC Staff 2018).[65]
- DOJ, as a part of the US Government's Executive Branch, advises other Executive Branch agencies both formally and informally on the issue of competition and data rights in the context of confidential deliberations within the government. DOJ also makes legislative recommendations and can file formal comments with other agencies. DOJ further collaborates with other agencies to ensure that any data privacy policies the government considers achieve the proper balance of protecting consumers, competition and law enforcement activities.

[61] James C. Cooper, Paul A. Pautler & Todd J. Zywicki, *Theory and Practice of Competition Advocacy at the FTC*, 72 ANTITRUST L.J. 1091, 1098 (2005); Maureen K. Ohlhausen, *Identifying, Challenging, and Assigning Political Responsibility for State Regulation Restricting Competition*, 2 *Comp. Pol'y Int.* 151 (2006). Daniel J. Gilman, *Advocacy*, SAGE ENCYCLOPEDIA OF POLITICAL BEHAVIOR 8 (Fathali M. Moghaddam, ed. 2017).

[62] Section 6 of the FTC Act, 15 USC 46, gives the Commission the authority to conduct investigations in the service of FTC enforcement actions, but also provides a more general authority to investigate and report on market developments in the public interest; and it gives the Commission the authority to make legislative recommendations based on those investigations. *Id.* at § 46(b), (f).

[63] Fed. Trade Comm'n Staff Comment Before the Office of the National Coordinator for Health Information Technology, regarding Its Draft Shared Nationwide Interoperability Roadmap for Health Information Technology Systems (Apr. 2015), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-office-national-coordinator-health-information-technology-regarding-its-draft/1504-roadmaphealth.pdf.

[64] FTC Staff Letter to the Department of Health and Human Services Concerning the 21st Century Cures Act: Interoperability, Information Blocking and the ONC Health IT Certification Program Rule (Mar. 2020), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-letter-department-health-human-services-concerning-21st-century-cures-act-interoperability/v190002hhsinfoblockingletter.pdf; FTC Staff Comment Before the Dep't of Health & Human Servs. Regarding the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (2019), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-department-health-human-services-regarding-21st-century-cures-act-interoperability/v190002_hhs_onc_info_blocking_staff_comment_5-30-19.pdf.

[65] FTC Staff Comment to the NTIA: Developing the Administration's Approach to Consumer Privacy (2018), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.