Antitrust Chronicle

SPRING 2015, VOLUME 2, NUMBER 2

Big Data
An Antitrust Perspective

CPI COMPETITION POLICY INTERNATIONAL

CPI COMPETITION POLICY INTERNATIONAL

CPI Antitrust Chronicle
May 2015 (2)

Big Data in a Competition Environment

Deborah Feinstein
U.S. Federal Trade Commission

www.competitionpolicyinternational.com

Big Data in a Competition Environment

Deborah Feinstein[1]

I. INTRODUCTION

The U.S. Federal Trade Commission ("FTC") is one agency with two missions: promoting competition and protecting consumers. Of course, competition and consumer protection laws have at their core the same fundamental goal: to promote consumer welfare through fair and vigorous competition unaltered by false, deceptive, or unfair tactics. In some circumstances, a particular set of facts may raise both competition and consumer protection issues. One area in which the two missions seem most likely to converge is in the world of big data.

To be clear, these would be distinct concerns. Despite calls to use the merger review process to improve privacy protections for consumers, the FTC continues to examine competition and consumer protection issues separately, examining the facts to determine if there is a potential violation of any law the FTC enforces. On the competition side, the inquiry remains focused on whether a merger is likely to create or enhance market power or facilitate its exercise, which can harm consumers by reducing competition along price and non-price dimensions such as quality or service.[2] We examine the extent to which the merging parties compete, who else competes, and whether others are likely to enter into the market. Since the decisions firms make about consumer privacy can lead to a form of non-price competition, the FTC has explicitly recognized that privacy can be a non-price dimension of competition.[3]

Although the FTC has yet to challenge a merger on the basis of a reduction in non-price competition over privacy protections, in some transactions involving data markets the FTC's challenges clearly lay the foundation for that potential case.

II. COMPETING WITH BIG DATA

The growing importance of data to modern business has long been apparent in the FTC's competition enforcement work. As early as 1996, when the FTC sought to undo a merger-to-monopoly in the field of salvage information management systems used by scrapyards and auto

[1] Deborah Feinstein is the Director of the FTC's Bureau of Competition. The views expressed herein are the author's and not necessarily those of the Commission or any Commissioner.

[2] U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines 2 (2010):

> Enhanced market power can also be manifested in non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation. Such non-price effects may coexist with price effects, or can arise in their absence. When the Agencies investigate whether a merger may lead to a substantial lessening of non-price competition, they employ an approach analogous to that used to evaluate price competition.

[3] Statement of the Commission, Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007).

repair shops,[4] we have examined the ways that firms compete using data as a product, an input, or a tool for making competitively significant decisions.

By way of illustration, consider the FTC's recent challenge to the merger of two firms providing rooftop aerial measurement services used by insurance companies to estimate repair costs for property damage claims. Prior to the development of these products, insurance adjusters or contractors would climb damaged roofs to obtain measurements—with obvious safety concerns and accuracy challenges. Based on our investigation of the likely competitive effects of the proposed merger, we heard that insurance companies prefer up-to-date, high-quality aerial images to calculate measurements of damaged buildings and to allow adjusters to identify attributes of the insured properties. The insurance companies also prefer that the measurement products integrate seamlessly with estimation software.

EagleView Technology Corporation was the self-proclaimed "industry standard," controlling approximately a 90 percent share of the market and serving most of the top 25 insurance carriers. EagleView had the most extensive aerial image library, while Verisk had the leading claims estimation software and a smaller proprietary aerial image library. From that position, Verisk entered the market to compete directly with EagleView and, within two years, Verisk had succeeded in winning significant customers away. Based on concerns about the elimination of that direct and growing competition through the proposed merger, the FTC filed an administrative complaint and authorized staff to seek a preliminary injunction to prevent the merger.[5] The parties abandoned their plans after the complaint was filed.

Mergers involving competing data providers can present unique, but not different, issues for competition analysis. For instance, market definition must account both for the dynamic nature of data, which must be updated and verified to retain its value, as well as the way that firms use data to compete. In some markets, data is the product—for instance, in the case of a database. In other markets, data is a key input, and firms compete to provide customized verification, analytics, or reporting to sophisticated customers. Using standard market definition analysis, the FTC has challenged mergers involving integrated drug information databases,[6] electronic public record services for law enforcement customers,[7] title plants,[8] and electronic systems used to estimate car repair costs.[9]

Similarly, entry conditions may be affected when incumbents have significant advantages over newcomers. For instance, the data involved may be publicly available, but existing firms

[4] *Automatic Data Processing, Inc.*, Dkt. No. 9282 (FTC complaint issued Nov. 14, 1996). ADP settled the charges by agreeing to divest the former AutoInfo assets and to grant the divestiture buyer an unrestricted license to its proprietary cross-indexed numbering system for auto parts. Nearly twenty years later, the FTC required divestitures to restore competition in the same market after the merger of two of the three leading providers. *Solera Holdings, Inc.,* No. C-4415 (FTC complaint issued Jul. 29, 2013).

[5] Fed. Trade Comm'n, Press Release, "FTC Challenges Verisk Analytic's Inc.'s Proposed Acquisition of EagleView Technology Corporation" (Dec. 16, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/12/ftc-challenges-verisk-analytics-incs-proposed-acquisition.

[6] *FTC v. Hearst Trust and First Databank, Inc.,* Civ. No. 1:01CV00734 (D.D.C. Apr. 4, 2001).

[7] *Reed Elsevier NV*, No. C-4257 (FTC complaint issued Sept. 15, 2008).

[8] *Fidelity National Financial, Inc.*, No. C-3920 (FTC complaint issued Jan. 12, 2000).

[9] *FTC v. CCC Holdings Inc.*, Civ. No. 1:08-CV-02043 (D.D.C. Nov. 26, 2008).

may have developed sophisticated analytic techniques or gained a reputation for reliability that makes it difficult for new entrants or fringe competitors to challenge established competitors.[10] In other cases, the data is not publicly available, and incumbents have a significant head start collecting and verifying data so that it would be difficult, costly, and time-consuming for a new firm to match the offerings of existing firms.[11] Sometimes, the databases serve as a platform for buyers and sellers to meet, such as is the case with real estate listing services,[12] in markets where network effects can be difficult to overcome.

Finally, the depth and scope of incumbents' data stores may have implications for innovation—or, more precisely, how new or existing firms can access and use data to develop new products. In *Nielsen Holdings/Arbitron*, the FTC alleged that the proposed merger would eliminate future competition to develop a national syndicated cross-platform audience measurement service.[13] According to the FTC, the two companies were best-positioned to develop this new product because they were the only firms with large, representative panels capable of reporting TV programming viewership, including individual demographic data such as age and gender information. To ensure that the merger did not eliminate emerging competition for these future products, the FTC required Nielsen to divest and license assets, including a royalty-free license to Arbitron's data for eight years, so that an FTC-approved buyer could successfully develop a service to compete with Nielsen's future product.

III. PRIVACY CONCERNS WITH CONSUMER DATA

With more and more data being collected about consumers—from their shopping habits to their sensitive health information—it was inevitable that the FTC would examine markets that include consumer data. In 2007, the FTC reviewed Google's acquisition of DoubleClick, which combined Google's user search data with DoubleClick's browsing data. After an extensive investigation, the FTC determined that Google and DoubleClick did not directly compete in any relevant market.

Moreover, the FTC examined a number of theories of potential harm due to leveraging, but found that the merger did not give Google an advantage that its rivals could not match. For instance, the staff determined that many of Google's most significant competitors in the ad intermediation market—firms the likes of Microsoft, Yahoo!, and TimeWarner—had access to their own unique data stores and popular search engines sufficient to compete vigorously against Google.[14]

As part of its merger review, privacy advocates urged the FTC to oppose the Google/DoubleClick transaction on the grounds that the combination of their respective data

[10] *See, e.g., CoreLogic, Inc*. No. C-4458 (FTC complaint issued Mar. 24, 2014) (national assessor and recorder bulk data collected from public records for real property transactions as well as local tax assessments available at local government offices).

[11] *See, Dun & Bradstreet*, Dkt. 9342 (FTC May 7, 2010) (administrative complaint settled with order requiring divestiture of updated database used to market educational materials for kindergarten through twelfth grade).

[12] For instance, the FTC has challenged a merger between two competing commercial real estate databases, citing the potential for unilateral anticompetitive effects. *CoStar Group, Inc.,* No. C-4368 (FTC Apr. 30, 2012).

[13] *Nielsen Holdings,* No. C-4439 (FTC complaint issued Sept. 30, 2013).

[14] Statement of the Commission, Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007).

sets of consumer information could be exploited in ways that threatened consumer privacy. In closing its investigation, the FTC explicitly declined to rely on its antitrust authority to intervene for reasons other than antitrust concerns. Similar appeals were made in the FTC's recent review of Facebook's acquisition of WhatsApp. In the Bureau of Competition, we reviewed the transaction using our standard approach, while staff in the Bureau of Consumer Protection ("BCP") considered the implications of the transaction on certain privacy issues, especially in light of Facebook's obligations contained in a 2011 FTC order that resolved allegations that Facebook had deceived consumers by failing to keep its privacy promises.[15]

Both Bureaus worked through their concerns, with different results. BCP focused on how the proposed transaction would affect the promises that WhatsApp had made to consumers about the limited nature of the data it collects, maintains, and shares with third parties—promises that exceeded the protections promised to Facebook users at the time the deal was announced. Although the transaction went forward as proposed, BCP concluded that it was appropriate to alert the companies about the privacy concerns raised and to assure the public that the protections under Section 5 and the FTC's Facebook Order would apply to WhatsApp data.[16]

Not every merger raises concerns about non-price competition, and only a few of those that do are likely to present concerns about a reduction in competition involving privacy protections. But even if a merger does not threaten to reduce competition in a meaningful way, the FTC will continue to use its consumer protection authority to ensure that companies live up to their obligations to protect the privacy of consumer data.

[15] *Facebook, Inc.,* No. C-4635 (FTC complaint issued Nov. 29, 2011).

[16] Letter from Jessica Rich, Dir. Bureau of Consumer Protection, FTC, to Erin Egan, Chief Privacy Officer, Facebook, Inc., and Anne Hoge, Gen. Counsel, WhatsApp Inc. (Apr. 20, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

CPI COMPETITION POLICY INTERNATIONAL

CPI Antitrust Chronicle

May 2015 (2)

Debunking the Myths over Big Data and Antitrust

Maurice E. Stucke & Allen P. Grunes

The Konkurrenz Group and
Data Competition Institute

Debunking the Myths over Big Data and Antitrust

Maurice E. Stucke & Allen P. Grunes[1]

I. INTRODUCTION

What are the implications of big data on competition policy? Some argue little, if any, and offer several reasons why big data is a passing fad.[2] We disagree. As we discuss here and elsewhere, competition law can play an important role in maximizing the benefits of a data-driven economy, while mitigating its risks.[3] Our aim here is to first address the competitive significance of Big Data and, second, take on ten myths downplaying Big Data's antitrust significance.

II. THE COMPETITIVE SIGNIFICANCE OF BIG DATA

Big data and the rise of data-driven business models have been, for several years, a hot topic in the business literature. Several years ago, a *McKinsey Quarterly* article asked, "Are you ready for the era of 'big data'?"[4] A *Harvard Business Review* article discussed how big data has the potential to transform traditional businesses: It "may offer them even greater opportunities for competitive advantage (online businesses have always known that they were competing on how well they understood their data)."[5] Indeed, the literature identifies five themes regarding companies acquiring and using big data:

1. Companies are increasingly adopting business models that rely on personal data as a key input. Data-driven business models, for example, involve two-sided markets; companies offer consumers free services with the aim of acquiring valuable personal data to assist advertisers to better target them with behavioral ads.

2. As the four "V"s of data—volume, velocity, variety, and value—increase, companies will undertake data-driven strategies to obtain and sustain a competitive advantage. Companies will offer products and services to harvest data that is not otherwise publicly available since the value of data may come from its variety. Data's value can increase through data fusion, which "occurs when data from different sources are brought into contact and new facts emerge."[6] Through data fusion, companies can identify and

[1] Maurice Stucke and Allen Grunes, both former attorneys with the U.S. Department of Justice Antitrust Division, are co-founders of The Konkurrenz Group and Data Competition Institute.

[2] *See, e.g.*, Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, ANTITRUST SOURCE (Dec. 2014), *available at* http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/dec14_tucker_12_16f.authcheckdam.pdf.

[3] Allen P. Grunes & Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, ANTITRUST SOURCE (Apr. 2015), *available at* http://ssrn.com/abstract=2600051.

[4] Brad Brown et al., *Are You Ready for the Era of "Big Data"?*, MCKINSEY Q. (Oct. 2011).

[5] Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARVARD BUS. REV. (Oct. 2012), *available at* https://hbr.org/2012/10/big-data-the-management-revolution/ar/1.

[6] 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 x (May 2014).

improve their profiles of individuals; better track their activities, preferences, and vulnerabilities; and better target them with behavioral advertising. Even for publicly available data, velocity can be critical—namely getting and analyzing the data in real-time or nearly real-time to outmaneuver rivals.[7] Consequently, companies will strive to acquire a "data advantage" over rivals.

3. The battle over data will spread to acquisitions. Given that data's value depends on its volume, variety, and how quickly the data is collected and analyzed, companies will increasingly focus on opportunities to acquire a data-advantage through mergers. According to one estimate, big-data related mergers doubled between 2008 and 2013—from 55 to 134.[8]

4. As data-driven mergers increase, one might expect—as in the TomTom/Tele Atlas merger[9] and Microsoft/Yahoo! joint venture[10]—the merging parties to raise as a defense data-driven efficiencies.

5. Businesses—to maintain their competitive advantage—will undertake data-driven strategies. Some tech firms, to maintain their dominance, will have strong incentives to: (i) limit their competitors' access to data, (ii) prevent others from sharing the data, and (iii) oppose data-portability policies that threaten their data-related competitive advantage. Companies will devise anticompetitive strategies to prevent rivals from accessing data (such as through exclusivity provisions with third-party providers) as well as to foreclose opportunities for rivals to procure similar data, such as making it harder for consumers to adopt other technologies or platforms.

As the Eleventh Circuit recently noted in *McWane*, a monopoly can violate section 2 of the Sherman Act when its exclusive dealing program deprives smaller rivals of "distribution sufficient to achieve efficient scale, thereby raising costs and slowing or preventing effective entry."[11] So too a dominant data-driven company can use exclusionary tactics to prevent rivals from achieving the minimum efficient scale.

Scale can be especially important in data-driven industries. Scale, as the U.S. Department of Justice ("DOJ") and European Commission ("EC") found in their Microsoft/Yahoo investigations, is unusually important in search and search advertising.[12] The recently released

[7] McAfee & Brynjolfsson, *supra* note 5.

[8] European Data Protection Supervisor, Report of Workshop on Privacy, Consumers, Competition and Big Data 1 (July 11, 2014), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdf.

[9] Case COMP/M.4854—TomTom/Tele Atlas, Comm'n Decision, 2008 O.J. (C237) 53–54, ¶¶ 245–250.

[10] Press Release, U.S. Dep't of Justice, Statement of the Department of Justice Antitrust Division on its Decision to Close its Investigation of the Internet Search and Paid Search Advertising Agreement Between Microsoft Corporation and Yahoo! Inc. (Feb. 18, 2010); Case COMP/M. 5727—Microsoft/Yahoo! Search Business Regulation, Comm'n Decision, 2010 O.J. (C 020/08).

[11] McWane, Inc. v. F.T.C., No. 14-11363, 2015 WL 1652200, at *19 (11th Cir. Apr. 15, 2015) (citing FTC findings).

[12] Maurice E. Stucke & Ariel Ezrachi, *When Competition Fails to Optimise Quality: A Look at Search Engines* (April 23, 2015), *available at* http://ssrn.com/abstract=2598128 or http://dx.doi.org/10.2139/ssrn.2598128.

portions of the U.S. Federal Trade Commission ("FTC") report by its Bureau of Competition staff in the Google investigation suggest the competitive significance of data. The report also alleged how Google used contractual restrictions to deny Microsoft critical scale, and thus impaired its ability to compete effectively in the markets for general search and search advertising.[13]

III. DEBUNKING THE MYTHS OF BIG DATA AND COMPETITION POLICY

The recent publication of the FTC Staff Report intensified the debate over the FTC's closing its investigation after Google committed to change some of its business practices.[14] When the EC recently issued its statement of objections over Google's degrading the quality of its search results by systematically favoring its own comparison shopping products in its general search results page, some shouted protectionism (without knowing the facts and evidentiary record that supported the EC's preliminary conclusion).

What is clear is that the EC's statement of objections will not end the matter. The EC is actively investigating other activities by Google, including "whether Google has illegally hindered the development and market access of rival mobile applications or services by requiring or incentivising smartphone and tablet manufacturers to exclusively pre-install Google's own applications or services."[15] The U.S. competition authorities, perhaps the DOJ,[16] will also likely investigate (if they are not already).

---

[13] Report from the FTC Bureau of Competition Staff to the Commission re Google Inc., at 94, 96, 98, 100, & 102. (Aug. 8, 2012), *available at* http://graphics.wsj.com/google-ftc-report/ [hereinafter "FTC Staff Report"]. A few caveats about this report, which the FTC released (mistakenly) under the Freedom of Information Act to the *Wall Street Journal*. First, only the Report's even pages were released, so the missing odd pages may have contained important qualifications. Second, other reports, including any prepared by the FTC economists and Google, were not released. Third, although the Competition Staff recommended the FTC to file a complaint, the Commissioners elected not to.

[14] FTC Press Release, Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search: Landmark Agreements Will Give Competitors Access to Standard-Essential Patents; Advertisers Will Get More Flexibility to Use Rival Search Engines (Jan. 3, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc. After portions of the FTC Staff Report were disclosed along with reports of meetings between White House and Google officials, the FTC Chair and two Commissioners responded, noting that the FTC conducted an "exhaustive" investigation of Google's internet search practices during 2011 and 2012:

> Based on a comprehensive review of the voluminous record and extensive internal analysis, of which the inadvertently disclosed memo is only a fraction, all five Commissioners (three Democrats and two Republicans) agreed that there was no legal basis for action with respect to the main focus of the investigation—search. As we stated when the investigation was closed, the Commission concluded that Google's search practices were not, 'on balance, demonstrably anticompetitive.'

Statement of Chairwoman Edith Ramirez, and Commissioners Julie Brill and Maureen K. Ohlhausen regarding the Google Investigation, March 25, 2015, https://www.ftc.gov/news-events/press-releases/2015/03/statement-chairwoman-edith-ramirez-commissioners-julie-brill. For Google's response, *see* http://graphics.wsj.com/google-ftc-report/.

[15] European Commission, Fact Sheet, Antitrust: Commission Opens Formal Investigation Against Google in Relation to Android Mobile Operating System, Apr. 15, 2015, *available at* http://europa.eu/rapid/press-release_MEMO-15-4782_en.htm.

[16] Diane Bartz & Dan Levine, *Google's Rivals Want the Justice Department to Probe Android*, REUTERS (Apr. 15, 2015).

As the recently disclosed portions of the FTC Staff Report and EC's investigation reflect, some members of the antitrust community are starting to appreciate the competitive benefits and risks of these data-driven strategies. Nonetheless, some are still propagating the following ten myths. For better antitrust enforcement, the debate must evolve beyond these myths:

A. Myth 1: Privacy Laws Serve Different Goals From Competition Law

Often privacy concerns do not implicate competition concerns. A landlord who secretly records a tenant's bedroom, for example, violates the common law privacy tort—intrusion upon seclusion—but not the competition laws. Likewise, some antitrust violations, like price-fixing cartels, generally do not raise privacy concerns.

But data-driven business strategies, at times, will raise both privacy and antitrust concerns. Data-driven mergers, like Facebook's acquisition of WhatsApp, for example, can potentially lessen non-price competition in terms of the array of privacy protections offered to consumers. Privacy, as a form of non-price competition, would arise if Google, the dominant search engine, were to acquire DuckDuckGo, which offers consumers greater privacy protection for their search queries.

Likewise, monopolies' data-driven exclusionary practices can hamper innovative alternatives that afford consumers greater privacy protection. Moreover, privacy competition—like other facets of non-price competition—already exists in other industries, but some dominant companies do not face the competitive pressure to improve quality along this dimension.

Thus one cannot quarantine privacy and competition concerns, unless one contorts the goals of competition policy to a narrow economic objective that few other antitrust practitioners and experts share.[17]

B. Myth 2: The Tools That Competition Officials Currently Use Fully Address All the Big Data Issues

The reality is that many of the current analytical economic tools do not address the Big Data issues. Competition authorities have good tools to assess price effects. But competition officials have less sophisticated tools to assess mergers' effects on non-price competition, including the impact on quality of free goods in two-sided markets and the degradation of privacy protection. The agencies' current tools can handle the egregious case, i.e., where the evidence is compelling that the companies are competing along non-price dimensions, such as privacy protection, and the merger is intended to substantially lessen this competition. But often the analysis of quality is less straightforward.[18] For example, the 1996 Telecommunications Act

[17] Scholars, as a 2013 symposium reveals, continue to debate over antitrust's goals, *see* Barak Orbach, *Foreword: Antitrust's Pursuit of Purpose*, 81 FORDHAM L. REV. 2151 (2013). At the symposium, even those who advocated an economic welfare objective disagreed whether welfare should reflect consumer welfare or total welfare, what those terms meant, and the extent to which it made any difference. Nor do the European scholars subscribe to a narrowly defined economic goal. *See* Ariel Ezrachi, *Sponge*, University of Oxford Centre for Competition Law and Policy Working Paper CCLP (L) 42; Oxford Legal Studies Research Paper No. 16/2015 (March 1, 2015), *available at* http://ssrn.com/abstract=2572028 or http://dx.doi.org/10.2139/ssrn.2572028.

[18] Ariel Ezrachi & Maurice E. Stucke, *The Curious Case of Competition and Quality*, J. ANTITRUST ENFORCEMENT (forthcoming 2015), draft *available at* http://ssrn.com/abstract=2494656 or http://dx.doi.org/10.2139/ssrn.2494656.

unleashed a merger wave in the commercial radio industry. In its consent decrees, the DOJ focused only on the paid advertising side, ignoring—to the detriment of consumers—the free "content" side.[19]

These tools will not magically appear but require effort. Some economists are already undertaking the task of creating them.

C. Myth 3: Market Forces Currently Solve Privacy Issues

The reality is that market forces are not solving privacy issues. Policymakers today acknowledge that privacy's notice-and-consent model is broken and ineffective. Consumers complain over their lack of control over their private data: "While Americans' associations with the topic of privacy are varied," a recent survey by the Pew Research Center found, the majority of adults "feel that their privacy is being challenged along such core dimensions as the security of their personal information and their ability to retain confidentiality."[20] In the survey, 91 percent of adults "'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies."[21]

D. Myth 4: Data-Driven Online Industries are Not Subject to Network Effects

Some data-driven industries are subject to network effects. Network effects, of course, are not always bad for consumers—think of telephones, the benefit of which increases as others use them. But network effects, at times, enable big firms to become bigger until they dominate the industry. Data-driven industries can be subject to several network effects, including:

- Traditional network effects, such as social networks like Facebook;
- Network effects involving the scale of data;
- Network effects involving the scope of data; and
- Network effects where the scale and scope of data on one side of the market affect the other side of the market (such as advertising).[22]

E. Myth 5: Data-Driven Online Markets Have Low Entry Barriers

As we discuss elsewhere, entry barriers for data-driven online industries are neither invariably low nor invariably high.[23] Each industry can differ. And entry barriers, once low, can increase due to network effects. One risk is that the economics of Big Data, as the OECD recently

---

[19] *See* Maurice E. Stucke & Allen P. Grunes, *Why More Antitrust Immunity for the Media Is a Bad Idea*, 105 NORTHWESTERN U. L. REV. 1399, 1411–12 (2011); Maurice E. Stucke & Allen P. Grunes, *Toward a Better Competition Policy for the Media: The Challenge of Developing Antitrust Policies that Support the Media Sector's Unique Role in Our Democracy*, 42 CONN. L. REV. 101, 124–25 (2009).

[20] Mary Madden, Pew Research Ctr., Public Perceptions of Privacy and Security in the Post-Snowden Era 3 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

[21] *Id.*

[22] See Stucke & Ezrachi, *supra* note 13.

[23] Grunes & Stucke, *supra* note 3, at 18.

observed, "favours market concentration and dominance."[24] Data-driven markets "can lead to a 'winner takes all' result where concentration is a likely outcome of market success."[25]

The fact that venture funds are investing in online startups does not mean entry barriers are necessarily low. An industry with high entry barriers can still have entrants. The Eleventh Circuit, for example, was unprepared to say that a competitor's "entry and growth foreclose a finding that McWane possessed monopoly power in the relevant market," especially given defendant's "overwhelming market share (90%), the large capital outlays required to enter the domestic fittings market, and McWane's undeniable continued power over domestic fittings prices."[26]

Moreover one has to examine in which particular markets the venture funds are investing. For example, few would likely fund a startup in the search market given Google's market share and Microsoft's reportedly investing in 2010 "more than $4.5 billion into developing its algorithms and building the physical capacity necessary to operate Bing."[27]

F. Myth 6: Data Has Little—If Any—Competitive Significance, Since Data Is Ubiquitous, Low Cost, and Widely Available

Beware of those who say this. Some companies take the position that data are like facts and argue that all data should be open. Some mapping companies, for example, might believe that the data needed to develop a map should be accessible to others. Other companies, however, treat their mapping data as proprietary and will not share. TomTom's arguments in the EC's investigation of the TomTom/Tele Atlas merger are particularly illustrative.

One question was whether Google or Microsoft could quickly enter the navigable digital map database market and become a significant competitor. TomTom argued yes: Both Google and Microsoft were customers of Tele Atlas and NAVTEQ, and both Google and Microsoft provided map services over the Internet. Thus, both tech companies, argued TomTom, "could use their technical knowledge and financial capabilities to upgrade their map databases to navigable quality by using feedback from their user communities."[28]

TomTom also claimed entry barriers had decreased for, among other things, "improved aerial photography, improved quality of satellite images and the possibility to use feedback from end-user communities."[29] The EC disagreed. Obtaining and processing this data, even for Google and Microsoft, would be costly and time-consuming.

TomTom raised another interesting argument, namely an entrant could avoid the cost of having to drive along every road to collect mapping data. Instead the entrant could rely on its subscribers to report this information as they drove along the roads. The EC again disagreed that entrants could lower the entry barriers through a positive feed-back loop with subscribers. Indeed, as the Office of Fair Trading ("OFT") later found in a merger between Google and Waze,

[24] OECD, Data-driven Innovation for Growth and Well-being: Interim Synthesis Report 7 (Oct. 2014).
[25] *Id.*
[26] *McWane*, 2015 WL 1652200, at *12.
[27] FTC Staff Report, *supra* note 14, at 76.
[28] EC TomTom Decision, *supra* note 9, at 23.
[29] *Id.* at 24.

it was Waze's inability to achieve sufficient scale of data that hindered its competitive significance in mapping services in the United Kingdom.[30] The OFT agreed that the more users supplied Waze with data on traffic conditions, the better Waze's turn-by-turn application became, and the more likely Waze would attract additional users. But this presented a chicken-and-egg dilemma. Users would not be attracted to mapping sites unless the quality was good, and the quality won't be good absent a sufficient amount of data from users.

Thus, companies currently spend considerable money and effort to acquire and analyze data and to maintain a data-related competitive advantage. If any company propagates this myth, ask it if it would be willing to license its consumer data to its competitors, and if so, at what price.

G. Myth 7: Data Has Little, If Any, Competitive Significance, as Companies Cannot Exclude Smaller Companies' Access to Key Data or Use Data to Gain a Competitive Advantage

Unlike Microsoft in the 1990s, today's dominant firms can benefit from the velocity of data to quickly identify and squelch nascent competitive threats in a process called "nowcasting."[31] Companies can use the velocity of data to discern trends well before others. In monitoring search queries, Google, for example, can predict flu outbreaks well before the government health agencies can. What then is there to prevent a dominant firm through similar nowcasting (such as watching for trends in its proprietary data from search queries, emails, etc.) from monitoring new business models in real time? The dominant firm can acquire these entrants before they become significant competitive threats or use other means to blunt their growth.

Thus, this use of big data would be as if the monopoly invented (or refined) a radar system to track competitive threats shortly after they take off from distant fields. The monopoly can intercept or shoot down the threats long before they become visible to regulators and others. Moreover, since the competitive threats are rather far away, the competition authorities, if they follow the OFT's logic in Google/Waze, will find the distant planes pose potential (yet speculative) threats, and will have insufficient evidence to prove that competition would likely be harmed. The monopolist, unlike the competition officials, is not concerned over the overall welfare effects of shooting down or intercepting the planes. It just intercepts or shoots them down.

H. Myth 8: Competition Officials Should Not Concern Themselves With Data-Driven Industries Because Competition Always Comes From Surprising Sources

In the long run, monopolists, like the rest of us, die. In the interim, dominant firms can stifle innovation. Consumers shouldn't suffer the harm from anticompetitive mergers and monopolistic abuses in the short-term because eventually a disruptive innovator will emerge.

---

[30] Office of Fair Trading, Completed Acquisition by Motorola Mobility (Google, Inc.) of Waze Mobile Ltd., ME/6167/13 (Dec. 17, 2013).

[31] Economists have adopted this term, originally used for near-term weather forecasts, to indicate a process where by using a large volume and variety of data they can monitor the state of the economy or other business trends in real time.

And this harm from anticompetitive data-driven strategies can be significant. The harm can go beyond higher advertising rates; it can include the loss of innovation, consumer choice, privacy, individual autonomy and freedom, and the citizens' trust in a market economy.

Such harm, the OECD recognized, can strike "the core values of democratic market economies and the well-being of all citizens."[32]

I. Myth 9: Competition Officials Should Not Concern Themselves With Data-Driven Industries Because Consumers Generally Benefit From Free Goods and Services

Consumers do not invariably benefit when services are "free," because these services are not actually free. Consumers often pay with their personal data and privacy. Because of the lack of transparency, consumers often don't realize how much they actually pay for these services. In fact economist Carl Shapiro, in a recent workshop, criticized the notion that because something is "free," it must be good for consumers. Prices can be positive, zero, or negative (where consumers are subsidized).[33]

In a January 2015 interview with MLex, European Competition Commissioner Margrethe Vestager discussed the linkages among data, privacy, and competition:

> Very few people realize that, if you tick the box, your information can be exchanged with others. . . . . Actually, you are paying a price, an extra price for the product that you are purchasing. You give away something that was valuable. I think that point is underestimated as a factor as to how competition works.[34]

Vestager made a similar point during her confirmation hearings before the European Parliament, where she described data as "the new currency of the Internet."[35] Vestager went on to note in the MLex interview:

> The more data you can collect, the more you know, the better product you can provide, but also the more powerful will you be towards others. . . . It isn't solely a competition issue. . . . It's very important for us to be able to say what is competition-related and what is an issue of privacy, ownership, data, [and] how you can be as secure on the net as you can be in the physical world.[36]

J. Myth 10: Consumers Who Use These Free Goods and Services Do Not Have Any Reasonable Expectation Of Privacy

Granted some people share a lot of personal details online. But generally we can infer consumers' privacy preferences from their choices only when:

---

[32] OECD Interim Synthesis Report, *supra* note 25, at 7.

[33] Daniel Donegan, Summary of Committee Program on Antitrust and Zero Price Products, The Price Point, Newsletter of the ABA Section of Antitrust Law, Pricing Conduct Committee, Winter 2015, at 16.

[34] MLex Interview: Margrethe Vestager (Jan. 2015), http://mlexmarketinsight.com/wp-content/uploads/2015/01/MLex-Interview-Vestager-22-01-151.pdf.

[35] James Kanter, *Antitrust Nominee in Europe Promises Scrutiny of Big Tech Companies*, N.Y. TIMES (Oct. 3, 2014).

[36] MLex Interview, *supra* note 35.

1. consumers are fully informed about their choice's benefits and costs (including privacy risks), and
2. the marketplace offers a competitive array of options that match actual privacy preferences.

That often isn't the case today. In competitive markets, consumers reign supreme. They wouldn't face a Hobson's choice of either using email (and suffer the privacy invasion of having their emails scanned to better target them with behavioral advertising) or writing letters. Many in the United States are frustrated, feeling they have lost control over their personal data. They are unaware of (i) who has access to their personal information, (ii) what data is being used, (iii) how and when the data is being used, and (iv) the privacy implications of the data's use.

IV. CONCLUSION

To be clear, we do not argue that Big Data is bad. Big Data is neither inherently good, evil, nor neutral. Its social value depends, among other things, on the industry and the purpose and effect of the data-driven strategy. Ultimately competition policy can play a key role in ensuring that citizens get the benefits of a data-driven economy, and in minimizing its risks.

CPI COMPETITION POLICY INTERNATIONAL

CPI Antitrust Chronicle
May 2015 (2)

The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework

Geoffrey A. Manne & R. Ben Sperry

International Center for Law and Economics

www.competitionpolicyinternational.com

The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework

Geoffrey A. Manne & R. Ben Sperry [1]

I. INTRODUCTION

Increasingly, people use the internet to connect with one another, access information, and purchase products and services. Along with the growth in the online marketplace have come concerns, as well, particularly regarding both the privacy of personal information as well as competition issues surrounding this and other data.

While concerns about privacy and data are not unique to the internet ecosystem, they are in some ways heightened due to the ubiquitous nature of information sharing online. While much of the sharing is voluntary, a group of scholars and activists have argued that several powerful online companies have overstepped their bounds in gathering and using data from internet users. These privacy advocates have pushed the U.S. Federal Trade Commission ("FTC") and regulators in Europe to incorporate privacy concerns into antitrust analysis.

We have undertaken a classification of the various proposed approaches to incorporating privacy into antitrust law elsewhere.[2] Here, we focus on the two most-developed theories: first, that privacy should be considered in mergers and other antitrust contexts as a non-price factor of competition; and second, that the collection and use of data can be used to facilitate anticompetitive price discrimination. In addition, we analyze the underlying conception of data as a barrier to entry that is a necessary precondition for supporting either proposed theory of harm.

II. PRIVACY AS AN ELEMENT OF NON-PRICE COMPETITION

Under antitrust law, according to some advocates, the best way to understand privacy is as a component of product quality. Thus some privacy advocates have argued that

> privacy harms can lead to a reduction in the quality of a good or service, which is a standard category of harm that results from market power. Where these sorts of harms exist, it is a normal part of antitrust analysis to assess such harms and seek to minimize them.[3]

---

[1] Executive Director and Associate Director, respectively, of the International Center for Law and Economics (ICLE). ICLE has historically received support from a broad coalition of groups interested in data, privacy, and competition policy issues, including Google, Amazon, and Facebook.

[2] *See* Geoffrey A. Manne & R. Ben Sperry, *The Law and Economics of Data and Privacy in Antitrust Analysis* (2014 TPRC Conference Paper, Aug. 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418779.

[3] *Behavioral Advertising: Tracking, Targeting, and Technology: Town Hall Before the FTC*, (Oct. 18, 2007) (testimony of Peter Swire, Professor, Moritz College of Law of the Ohio State University), *available at* http://www.americanprogress.org/issues/regulation/news/2007/10/19/3564/protecting-consumers-privacymatters-in-antitrust-analysis/.

The Horizontal Merger Guidelines have long recognized that anticompetitive effects may "be manifested in non-price terms and conditions that adversely affect customers."[4] But this notion, while largely unobjectionable in the abstract, still presents significant problems in actual application.

First, product quality effects can be extremely difficult to distinguish from price effects. Quality-adjusted price is usually the touchstone by which antitrust regulators assess prices for competitive effects analysis. Disentangling (allegedly) anticompetitive quality effects from simultaneous (neutral or pro-competitive) price effects is an imprecise exercise, at best. For this reason, proving a product-quality case alone is very difficult and requires connecting the degradation of a particular element of product quality to a net gain in advantage for the monopolist.

Second, invariably product quality can be measured on more than one dimension. For instance, product quality could include both function and aesthetics: A watch's quality lies in both its ability to tell time as well as how nice it looks on your wrist. A non-price effects analysis involving product quality across multiple dimensions becomes exceedingly difficult if there is a tradeoff in consumer welfare between the dimensions. Thus, for example, a smaller watch battery may improve its aesthetics, but also reduce its reliability. Any such analysis would necessarily involve a complex and imprecise comparison of the relative magnitudes of harm/benefit to consumers who prefer one type of quality to another.

A. Privacy Advocates Have Failed to Prove a Product Quality Case

The understanding of how quality-adjusted price may be affected by monopolization of data or a merger of entities with large quantities of data requires considerably more analysis than that offered by privacy advocates thus far.

In the merger context (where most of the antitrust-relevant concerns about privacy-as-product-quality have been raised), one claim is that the accumulation of "too much" information about too many consumers is itself (or perhaps will inevitably lead to) a degradation of quality affecting the merging parties' products.

But that "problem" is almost certainly fully internalized by individual consumers. Consumers, with the assistance of consumer protection agencies like the FTC itself, are generally able to assess the risks of disclosure or other misuse of their information, and to assess the expected costs to themselves if such misuse should occur. Unless the collection of data on other people increases the uncertainty of this risk assessment, or makes harm to the individual consumer more likely (and it is difficult to see why either would likely be the case), it is difficult

[4] *See, e.g.*, 2010 Merger Guidelines, sec. 1 ("Enhanced market power can also be manifested in non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation. Such nonprice effects may coexist with price effects, or can arise in their absence."); 1997 Merger Guidelines, sec. 0.1 & note 6 ("The unifying theme of the Guidelines is that mergers should not be permitted to create or enhance market power or to facilitate its exercise. Market power to a seller is the ability profitably to maintain prices above competitive levels for a significant period of time. . . Sellers with market power also may lessen competition on dimensions other than price, such as product quality, service, or innovation.").

to see why a company's mere possession of private information about other people is of much concern to any particular consumer.

The size of a database (i.e., the number of consumers on whom data is collected) doesn't seem like a particularly relevant aspect of product quality in and of itself, and for each consumer the "problem" of a large concentration of information being accumulated in a single company is seemingly insignificant. Meanwhile, to the extent that collection of data from more consumers is a function of increasing network effects, such accumulations of data are almost certainly more likely to correlate with improvements in product quality rather than degradations.

While an increased amount of aggregated data at the disposal of one entity is not likely a significant harm in and of itself, it is surely the case that specific privacy policies that may affect a company's treatment of a consumer's own information may be relevant to his assessment of product quality. Particularly where consumers are paying a zero price (as search engine users and advertising consumers do), non-price competition, including over privacy policies, may be the only source of cognizable effects.

But in that case it must still be shown that a monopolist would have the ability and the incentive (and, in the case of a merger, that these would be merger-specific) to curtail privacy protections as a means of exercising its monopoly power. But this seems unlikely. As FTC Commissioner Joshua Wright noted in a recent speech on the internet of things:

> Without any analytical lens through which to interpret [the fact that some companies possess large volumes of data], frankly, so what? . . . [Y]es, that generation of data has implications for both the benefits to consumers from the exchange of data and the risks of specific harms. But the fact that there are millions of data points is not—in and of itself—a privacy risk. What is required to inform policy is not a general suspicion of large data sets and their uses, but rather a more nuanced analysis at least acknowledging the tradeoffs involved for consumers at the margin.[5]

In the normal case, a monopolistic firm would have an incentive to degrade quality if doing so would lower its costs and the demand elasticity were smaller for downward adjustments in quality than for corresponding increases in price. But in the case of privacy protections—where, for example, one "harm" might be the maintenance of personal information on a firm's servers for extended periods without deletion—it would seem that a firm might actually incur more cost in degrading (storing information for longer) than in maintaining (deleting cumbersome information from limited storage space) privacy.

At the same time, alleged harms arising from increased sharing of data with third parties (typically advertisers) is necessarily ambiguous, at best. While some consumers may view an increase in data sharing as a degradation of quality, the same or other consumers may also see the better-targeted advertising such sharing facilitates as a quality improvement, and in some cases "degraded" privacy may substitute for a (pro-competitive) price increase that would be far less attractive.

---

[5] Remarks of Joshua D. Wright, U.S. Chamber of Commerce, *How to Regulate the Internet of Things Without Harming its Future: Some Do's and Don'ts*, at 11-12 (May 21, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/644381/150521iotchamber.pdf.

Similarly, claims that concentration will lead to a "less-privacy-protective structure"[6] for online activity are analytically empty. One must make out a case, at minimum, that a move to this sort of structure would reward the monopolist in some way, either by reducing its costs or by increasing revenue from some other source. Absent a coordinated effects argument (which has not to our knowledge ever been raised), increased data concentration alone would seem to be insufficient; unilateral effects must be shown for such a merger to be anticompetitive. There appears to be little incentive for a monopolist to lower quality on its own, unless the barriers to entry are so high that no possible alternatives could exist.

In short, proponents of the theory of product-quality harm arising from monopolization of data need to make out an economically sound case for why the feared privacy degradation would occur at all, or ever be anticompetitive if it did, and this they have not done.

B. Most Consumers Prefer "Free and Useful" to "More Private"

As suggested above, on top of the difficulty in parsing out price effects from product quality effects, there seems also to be a tradeoff in consumer perception of product quality from increased data collection between the algorithmic improvements it may facilitate and the (posited) privacy harms it entails. A decrease in privacy protection is not simply a transfer from consumers to producers creating the famous deadweight loss of antitrust textbooks. Rather, the collection and use of larger amounts of information by a company like Google has the ability to improve the quality of Google's products, whether by improving the relevance of its search results or the successful targeting of its ads. In either case, improving product quality while maintaining a constant zero price—i.e., decreasing quality-adjusted price—is not normally an antitrust injury.

In fact, as we describe in more detail below, several critics assert that the collection and use of more data amounts to a data barrier to entry precisely because it improves the quality of Google's algorithm in ways that competitors can't replicate. While there may not be a one-to-one correlation between data collection and product quality, it certainly cannot be said that there is an obvious decrease in quality for consumers when more data is collected, either.

The question of antitrust-relevant product quality really comes down to the relative numbers of, and magnitude of harm to, consumers who prefer more privacy protection versus those who prefer a better search experience and/or a lower monetary price. Most of the available data suggests that the vast majority of consumers value privacy quite a bit less than they do other product attributes, including price.[7] For instance, revealed preferences in search and elsewhere

[6] Swire, *supra* note 3 ("For these individuals, their consumer preferences are subject to harm if standard online surfing shifts to a less privacy-protective structure due to a merger or dominant firm behavior. In essence, consumers "pay" more for a good if greater privacy intrusions are contrary to their preferences. Under standard economic analysis, and standard antitrust analysis, harm to consumer preferences should be part of the regulatory homework for the competition agencies—such harms should be considered along with other harms and benefits from a proposed merger.").

[7] *See, e.g.*, Alastair R. Beresford, Dorothea Kübler, & Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* (SFB 649 Discussion Paper 2011-010, 2011), *available at* http://edoc.hu-berlin.de/series/sfb-649-papers/2011-10/PDF/10.pdf; Jens Grossklags & Alessandro Acquisti, *When 25 Cents is too much: An Experiment on*

suggest that viewing a targeted ad (to access a news article, for example) amounts to a much lower "price" (i.e., psychic burden) on most people than does paying even just a few cents per month for an otherwise identical, ad-free experience. By the same token, consumers almost always choose free (ad-supported) apps over the 99 cent alternative without ads.[8]

To make out an antitrust case based on such privacy "harms," antitrust regulators would have to compare the magnitude of the harms to what appears to be a small group of privacy-sensitive consumers (who have not otherwise protected themselves by use of marketplace tools like track-blockers or by use of the opt-out options provided by major ad networks and data brokers) to the benefits received by the supermajority of consumers who are less privacy-sensitive. Beside the enormous difficulty of actually performing such an analysis, it seems extraordinarily unlikely that the harms would outweigh the benefits on net.

Unfortunately for proponents of a non-price competition theory of privacy and antitrust, not only is there no obvious reason why monopolists would have an incentive to degrade privacy, there is also no necessary (or even likely) connection between more data collection and use and harm to consumer welfare.

III. PRICE DISCRIMINATION AS A PRIVACY HARM

If non-price effects cannot be relied upon to establish competitive injury (as explained above), then what can be the basis for incorporating privacy concerns into antitrust? One argument is that major data collectors (e.g., Google and Facebook) facilitate price discrimination.[9]

The argument can be summed up as follows: Price discrimination could be a harm to consumers that antitrust law takes into consideration. Because companies like Google and Facebook are able to collect a great deal of data about their users for analysis, businesses could segment groups based on certain characteristics and offer them different deals. The resulting price discrimination could lead to many consumers paying more than they would in the absence of the data collection. Therefore, the data collection by these major online companies facilitates price discrimination that harms consumer welfare.

This argument misses a large part of the story, however. The flip side is that price discrimination could have benefits to those who receive lower prices from the scheme than they would have in the absence of the data collection, a possibility explored by the recent White House Report on Big Data and Differential Pricing.[10]

Willingness-To-Sell and Willingness-To-Protect Personal Information, in PROCEEDINGS OF THE SIXTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2007), *available at* http://weis2007.econinfosec.org/papers/66.pdf.

[8] Mary Ellen Gordon, *The History of App Pricing, and Why Most Apps are Free*, THE FLURRY BLOG (Jul. 18, 2013), http://blog.flurry.com/bid/99013/The-History-of-App-Pricing-And-Why-Most-Apps-Are-Free.

[9] *See* Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 850, 865-73, *available at* http://open.wmitchell.edu/cgi/viewcontent.cgi?article=1568&context=wmlr.

[10] EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, BIG DATA AND DIFFERENTIAL PRICING 17 (Feb. 2015), *available at* https://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf ("if historically disadvantaged groups are more price-sensitive than the average consumer, profit-maximizing differential pricing should work to their benefit").

While privacy advocates have focused on the possible negative effects of price discrimination to one subset of consumers, they generally ignore the positive effects of businesses being able to expand output by serving previously underserved consumers. It is inconsistent with basic economic logic to suggest that a business relying on metrics would want to serve only those who can pay more by charging them a lower price, while charging those who cannot afford it a larger one. If anything, price discrimination would likely promote more egalitarian outcomes by allowing companies to offer lower prices to poorer segments of the population—segments that can be identified by data collection and analysis.

If this group favored by "personalized pricing" is as big as—or bigger than—the group that pays higher prices, then it is difficult to state that the practice leads to a reduction in consumer welfare, even if this can be divorced from total welfare. Again, the question becomes one of magnitudes that has yet to be considered in detail by privacy advocates.

Further, this analysis fails to consider the dynamic efficiencies of price discrimination. In a static model of third-degree price discrimination, some buyers receive lower prices (and purchase higher quantities), while other buyers receive higher prices (and purchase lower quantities). Thus, the net impact of price discrimination on output is ambiguous.[11] But in a dynamic model, price discrimination may often be pro-competitive because the prospect of higher profits provides incentives for entry and allows for additional investments in innovation, increasing product variety, expanding retail outlets, or research and development.[12] As mentioned above, price discrimination may allow for increased competition to all consumers, including previously unreached and poorer consumers, another pro-competitive outcome.[13] Contrary to the received wisdom,[14] economists have noticed that price discrimination is present in even competitive markets.[15]

Under a proper error cost framework, courts and antitrust regulators should refrain from declaring conduct anticompetitive unless the likelihood of pro-competitive outcomes is demonstrably low.[16] In this case, it appears very difficult for antitrust regulators to differentiate positive price discrimination from negative price discrimination, and it seems unlikely that the price discrimination "facilitated" by major data collectors is anticompetitive.

For instance, Google analytics is used by many businesses, any number of which compete with one another in the same markets to offer the best deals to consumers through targeted advertising. It seems just as—if not more—likely that Google is increasing consumer welfare by helping businesses find consumers interested in their products and by serving up more relevant

[11] *See, e.g.*, Joshua D. Wright, *Missed Opportunities in Independent Ink*, CATO SUPREME COURT REV. 2005-2006, at 348, *available at* http://object.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2006/9/wright.pdf.

[12] *Id.* at 350.

[13] *Id.*

[14] *See* William M. Landes & Richard A. Posner, *Market Power in Antitrust Cases*, 94 HARV. L. REV. 937, 977 (1981).

[15] *See, e.g.*, 70 ANTITRUST L. J. 593 (2003) (symposium articles discussing competitive price discrimination).

[16] *See* Frank H. Easterbrook, *The Limits of Antitrust*, 63 TEX. L. REV. 1 (1984). The error cost model is well-accepted in the antitrust law and economics literature. *See, e.g.*, Geoffrey A. Manne & Joshua D. Wright, *Innovation and the Limits of Antitrust*, 6 J. COMPETITION L. & ECON. 153 (2010).

advertisements to those consumers—thus increasing the amount of positive-sum transactions overall.

Finally, price discrimination as a harm in itself is rarely antitrust-relevant. The Robinson-Patman Act, a New Deal-Era amendment to the Clayton Act's prohibitions on price discrimination, does not extend to price discrimination against end consumers.[17] Further, the Robinson-Patman Act has fallen into disrepute because of the outdated economic model it was based upon, leading the Antitrust Modernization Commission to call for its repeal in 2007:

> The Robinson-Patman Act does not promote competition…. Instead, the Act protects competitors, often at the expense of competition that otherwise would benefit consumers, thereby producing anticompetitive outcomes. The Act prevents or discourages discounting that could enable retailers to lower prices to consumers. "The chief 'evil' condemned by the Act [is] low prices, not discriminatory prices." The Act thus reflects "faulty economic assumptions" and a significant "misunderstanding of the competitive process."[18]

Price discrimination, even if facilitated by data, is not an antitrust harm a court or competition agency is likely to accept.

IV. DATA BARRIER TO ENTRY

Either of these theories of harm is predicated on the inability or difficulty of competitors to develop alternative products in the marketplace—the so-called "data barrier to entry." The argument is that upstarts do not have sufficient data to compete with established players like Google and Facebook, which in turn employ their data to both attract online advertisers as well as foreclose their competitors from this crucial source of revenue. There are at least four reasons to be dubious of such arguments:

1. Data is useful to all industries, not just online companies;
2. It's not the amount of data, but how you use it;
3. Competition online is one click or swipe away; and
4. Access to data is not exclusive.

A. First, Data is Useful to All Industries—This is Not a New Phenomenon Particular To Online Companies

The market for data, even if narrowly described as data for targeted advertising, is much broader than the online world. Offline retailers have long used data about consumers to better serve them. Through devices like coupons and loyalty cards (to say nothing of targeted mailing lists and the age-old practice of data mining check-out receipts), brick-and-mortar retailers can track purchase data and better serve consumers.[19] Not only do consumers receive better deals for

[17] *See* Newman, *Costs of Lost Privacy*, *supra*, at 875-76 n.107-08.

[18] *See* ANTITRUST MODERNIZATION COMMISSION, REPORT AND RECOMMENDATIONS 317 (Apr. 2007), *available at* http://govinfo.library.unt.edu/amc/report_recommendation/amc_final_report.pdf (internal citations omitted).

[19] *See, e.g.*, Nancy Kross, *Big Data Analytics Revolutionizing The Way Retailers Think*, BIDNESS ETC (Jun. 26, 2014), http://www.bidnessetc.com/business/big-data-analytics-revolutionizing-the-way-retailers-think/; Dianne

using them, but retailers also learn what products to stock and advertise, and when and on what products to run sales.

And of course there is a host of other uses for data, as well, including security, fraud prevention, product optimization, risk reduction to the insured, knowing what content is most interesting to readers, etc. The importance of data stretches far beyond the world of online advertising, and far beyond mere retail uses more generally.

B. Second, It's Not the Amount of Data That Leads to Success But How You Use It

Information is important to companies because of the value that can be drawn from it, not for the inherent value of the data itself. Companies don't collect information about you to stalk you, but to better provide you with goods and services.

Consider companies like Uber, Lyft, and Sidecar that had no customer data when they began to challenge established cab companies that did possess such data. If data were really so significant, they could never have competed successfully. But Uber, Lyft, and Sidecar have been able to effectively compete because they built products that users wanted to use[20]—they came up with an idea for a better mousetrap. The data they have accrued came after they innovated, entered the market, and mounted their successful challenges—not before.

In reality, those who complain about data facilitating unassailable competitive advantages have it backward. Companies need to innovate to attract consumer data, otherwise consumers will switch to competitors (including both new entrants and established incumbents). As a result, the desire to make use of more and better data drives competitive innovation, with manifestly impressive results: the continued explosion of new products, services, and apps is evidence that data is not a bottleneck to competition but a spur to drive it.

C. Third, Competition Online Is One Click or Thumb Swipe Away; That Is, Barriers to Entry and Switching Costs Are Low

Somehow, in the face of alleged data barriers to entry, competition online continues to soar, with newcomers constantly emerging and triumphing. This suggests that the barriers to entry are not so high as to prevent robust competition.

Again, despite the supposed data-based monopolies of companies like Facebook and Google, there exist powerful competitors in the marketplaces they compete in. Among many examples:

- If consumers want to make a purchase, they are more likely to do their research on Amazon than Google.[21]

Heath, *How Panera Uses Rewards Card to Increase Customer Loyalty & Attract Customers*, ANALYST DISTRICT (Nov. 4, 2011), http://www.analystdistrict.com/2011/11/panera-increase-customer-loyalty.html.

[20] *See* Karen Mathews & Verena Dobnick, *Uber Cars in New York Now Outnumber Yellow Cabs*, HUFFINGTON POST (Mar. 19, 2015), http://www.huffingtonpost.ca/2015/03/19/new-york-citys-storied-y_n_6900980.html.

[21] *See* Rolfe Winkler, *Amazon vs. Google: It's a War for Shopping Search*, WALL ST. J. (Dec. 13, 2013), http://www.wsj.com/articles/SB10001424052702304173704579265421113585650.

- Google flight search has failed to seriously challenge—let alone displace—its competitors, as critics feared. Kayak, Expedia, and the like remain the most prominent travel search sites—despite Google having literally purchased ITA's trove of flight data and data-processing acumen.[22]
- Pinterest, one of the most highly valued startups today,[23] is now a serious challenger to traditional search engines when people want to discover new products.
- Likewise, Amazon recently launched its own ad network, "Amazon Sponsored Links," to challenge other advertising players.[24]

Even assuming for the sake of argument that data creates some barrier to entry, there is little evidence that consumers cannot or will not readily switch to a range of competitors. While there are sometimes network effects online, as with social networking, history still shows that people will switch. MySpace was considered a dominant network until it made a series of bad business decisions and everyone ended up on Facebook instead.[25] Similarly, internet users can and do use Bing, DuckDuckGo, Yahoo, and a plethora of more specialized search engines on top of and instead of Google. And Google itself was once an upstart new entrant that replaced once-household names like Yahoo and AltaVista.[26]

D. Fourth, Access to Data is Not Exclusive

Critics have compared Google to Standard Oil and argued that government authorities need to step in to limit Google's control over data.[27] But to say that data is like oil betrays a serious misunderstanding. If Exxon drills and extracts oil from the ground, that oil is no longer available to BP. Data is not finite in the same way. Google knowing my birthday doesn't limit the ability of Facebook to know my birthday, as well. While databases and the processes used to create and make use of them may be proprietary, the underlying data is not. And what matters more than the data itself is how well it is analyzed.

This is especially important when discussing data online, where multi-homing is ubiquitous. Multi-homing can be accomplished by tools like the friend-finder feature on WordPress to search out Facebook friends, Google connections, and Twitter followers who also

---

[22] *See* Rob Pegoraro, *Remember When Google Was Going to Annex the Travel-Search Industry?*, PROJECT-DISCO (Jun. 4, 2013), http://www.project-disco.org/competition/060413-remember-when-google-was-going-to-annex-the-travel-search-industry/.

[23] *See* Yoree Koh, *Pinterest Valued at $11 Billion After Latest Funding*, WALL ST. J. (Mar. 16, 2015), http://www.wsj.com/articles/pinterest-raises-367-million-at-11-billion-valuation-1426538379.

[24] *See* Mark Sullivan, *Amazon's new ad network has a secret weapon against Google AdWords: shopping data*, VENTURE BEAT (Aug. 23, 2014), http://venturebeat.com/2014/08/23/amazon-will-use-shopping-data-to-target-ads-better-than-googles-adwords/.

[25] *See So What "Really" Happened To and What's Happening With MySpace?*, NETWEEK (May 17, 2013), http://www.thesba.com/2013/05/17/so-what-really-happened-to-and-whats-happening-with-myspace/.

[26] *See* Geoffrey A. Manne & William Rinehart, *The Market Realities that Undermined the FTC's Antitrust Case Against Google*, 2013 HARV. J. L. & TECH. 1, 14-17 (Online Paper Series, July 2013), *available at* http://jolt.law.harvard.edu/antitrust/articles/ManneRinehart.pdf.

[27] Nathan Newman, *Taking on Google's Monopoly Means Regulating Its Control of User Data*, HUFFINGTON POST (Sept. 24, 2013), http://www.huffingtonpost.com/nathan-newman/taking-on-googles-monopol_b_3980799.html.

use the site for blogging. Most popular platforms make such APIs available to all comers, effectively permitting the transfer of large swaths of data to competitors.

Moreover, the recently announced merger between Verizon and AOL may be a harbinger of yet another source of competition for data for online advertising. As a recent *New York Times* story details:

> People in the ad-tech industry said that in buying AOL, Verizon's immediate goal may be to marry its data about customers to AOL's capacity to serve ads to increase this sort of relevancy.
>
> "I think AOL was a little on their back foot on mobile," said Ari Paparo, chief executive of an ad technology company called Beeswax. He added that the most successful companies with mobile ads tended to be those that knew a lot about their customers—that explains why Google and Facebook, which have close to perfect insight into what we do online, are such powerhouses.[28]

Mobile ISPs like Verizon already have access to considerable data about consumers, likely at least comparable to what Google and Facebook have. What's more, mobile ISPs have uniquely good access to location data, which is increasingly the coin of the realm in a world where the most important and valuable consumer interactions are shifting to mobile. As suggested above, if there were a "barrier" to Verizon competing with other online platforms, it almost certainly arose from the absence of an effective use of its data, not from any lack of data itself.

IV. CONCLUSION

Privacy advocates have thus far failed to make their case. Even in their most plausible forms, the arguments for incorporating privacy and data concerns into antitrust analysis do not survive legal and economic scrutiny. In the absence of strong arguments suggesting likely anticompetitive effects, and in the face of enormous analytical problems (and thus a high risk of error cost), privacy should remain a matter of consumer protection, not of antitrust.

[28] Farhad Manjoo, *For Verizon and AOL, Mobile is a Magic Word*, THE NEW YORK TIMES (May 12, 2015), http://www.nytimes.com/2015/05/13/technology/verizons-data-trove-could-help-aol-score-with-ads.html.

CPI COMPETITION POLICY INTERNATIONAL

CPI Antitrust Chronicle

May 2015 (2)

Big Data as a Barrier to Entry

Robert P. Mahnke
eBay Inc.

www.competitionpolicyinternational.com

Big Data as a Barrier to Entry

Robert P. Mahnke[1]

So-called "big data" has been a technological development for some time, and lately it has matured into a phenomenon that competition lawyers have noticed. Mindful of the vast quantities of data that some companies are amassing, some argue that access to data can be a barrier to entry in online markets, protecting incumbents from competition. However, Geoffrey Manne & Ben Sperry recently argued "the notion of data as an antitrust-relevant barrier to entry is simply a myth."[2] Manne & Sperry have it wrong: The fact that "big data" can be an antitrust-relevant barrier to entry has been well established.

At the outset, one problem is that the term "big data" seems to mean different things to different people. Darren Tucker & Hill Welford emphasize the extent to which once-sophisticated tools are increasingly ubiquitous: "Big data is everywhere. … Big data is used by organizations of all sizes. Small businesses, entrepreneurs, and government agencies, in addition to large companies, are avid users of big data."[3] Used in this way, "big data" is "bigger" than yesterday's data, but what gets lost are the profound differences among some of these different users.

Those who are concerned about big data as a competition problem have something different in mind. Some firms are amassing data at a completely different scale. To take one public example, Google recently opened a new server farm in Oregon, "a massive, 164,000-square-foot building" that cost $600 million.[4] According to the *Oregonian*, "Google now has data centers all over the country and around the world." Small businesses and investors cannot afford such investments, nor can many large companies. When big data gets that big, most market participants will be excluded, and competition problems will be more likely.

Manne & Sperry suggest that data matters in offline markets as well. As more of us carry and use smartphones and tablets at all hours, the distinction between online and offline business will seem increasingly archaic, but, still, Manne & Sperry are not wrong. So, they say, the notion

---

[1] Global Competition Counsel at eBay Inc.; formerly Trial Attorney at the U.S. Department of Justice, Antitrust Division. The views here are those of the author alone and should not be attributed to eBay

[2] Geoffrey Manne & Ben Sperry, *Debunking the Myth of a Data Barrier to Entry for Online Services*, TRUTH ON THE MARKET (March, 2015), *available at* http://truthonthemarket.com/2015/03/26/debunking-the-myth-of-a-data-barrier-to-entry-for-online-services/. *See also* Darren S. Tucker & Hill B. Welford, *Big Mistakes Regarding Big Data*, ANTITRUST SOURCE (December 2014) ("Online markets are notable for their low entry barriers and typically do not require big data for entry."); Daniel O'Connor, *Is Big Data an Entry Barrier? What Tinder Can Tell Us*, (April 2, 2015), *available at* http://www.project-disco.org/competition/040215-big-data-entry-barrier-tinder-can-tell-us/ ("However plausible this argument sounds, a review of the short history of the Internet economy … seems to cast doubt on the soundness of the theory."); Andres V. Lerner, *The Role of 'Big Data' in Online Platform Competition*, *available at* http://ssrn.com/abstract=2482780 (August 26, 2014).

[3] Tucker & Welford, *Id.*

[4] Mike Rogoway, *Google opens new, $600 million Oregon data center*, (April 9, 2015), *available at* http://www.oregonlive.com/silicon-forest/index.ssf/2015/04/google_opens_new_oregon_data_c.html.

that companies like Google or Facebook could have "a monopoly on data is silly." Well, this is patently true, but not because offline firms have data too. Data are not a commodity. What Google knows about where your phone went last weekend is not like what Facebook knows about your circle of friends from high school.

Axiomatically, product markets are comprised of goods which are reasonable substitutes for each other. Data is no such thing, and so it makes no sense to talk about a product market in "data." There are so many, many, kinds of data. It very well may be the case that Tinder, to take an example discussed by Daniel O'Connor, did not face data-related barriers to entry when it started to compete with other dating services, but that hardly dictates that the same will be true in other product markets. Competitive markets may all be alike, at least in theory, but every uncompetitive market is uncompetitive in its own way.

Manne & Sperry further argue that it doesn't really matter how much data a company has; what matters is what they do with it when they design their products and services. Doubtless this can be true, and Manne & Sperry offer examples. But the online economy is incredibly diverse, featuring robust competition and terrific innovation in some corners, and dominant incumbents with remarkably durable market power in others. There is no single internet business plan. Many start-ups have been successful despite not (yet) having their own data because they have persuaded users to give it to them. Web 2.0 and social media provide many examples.

But not every industry can be won with a social model. If there is strong competition in some markets, that does not mean that there are no barriers to entry in others. And past performance is no guarantee of future results. Even if "Google achieved success over other search engines by conceiving of a better way of matching users queries to relevant websites,"[5] as Daniel O'Connor says, the information it has now compiled about what many of us have searched for and found useful cannot be easily replicated.

It is true that data are not like oil, in that Google and Facebook (for example) both can have the same data. (Though they also surely have many data the other does not, given the different ways that they interact with their users.) Indeed, in online businesses, this is a commercial reality. For example, shopping-comparison sites get their data about products and prices from merchants. The specifications of, say, a camera do not change when it is sold in different places. And merchants find it burdensome to create and deliver different data about their goods, so online shopping comparison sites tend to have the same product data and to compete in other ways—e.g., by generating their own unique content like product reviews.

But while two parties *could* have the same data, that hardly means that in any given industry they *will* have it. There are data, and then there are data. Some businesses are successful and valuable because they have access to data that others cannot easily obtain. For example, Craigslist. When other companies have attempted to scrape its listings, Craigslist has tried to stop

[5] Tom Hornby, *The Rise of Google, Beating Yahoo at Its Own Game*, LOWEND MAC (2013), hyperlink in the original, *available* at http://lowendmac.com/2013/the-rise-of-google-beating-yahoo-at-its-own-game/.

them, with success.[6] Is it impossible for anyone to compete with Craigslist in its core business? Maybe not, but anyone trying faces a substantial barrier to entry. Does every online or digital market work like this? Of course not, but some do.

Blanket assertions about the competitive dynamics of data do not illuminate the circumstances of specific markets. We have a concrete example of barriers to entry in data markets, a merger that led to precedents on both sides of the Atlantic. In 2007, Thomson announced it would acquire Reuters. Both companies offered, among other things, terminals to traders and other financial professionals. It was reported at the time that the merger was intended to enable the combined company to better compete with Bloomberg and its eponymous terminal. In essence, Thomson and Reuters offered bundles of financial data.

Both the U.S. Department of Justice ("DOJ") and the European Commission's Directorate General for Competition ("DG Comp") investigated the acquisition, and eventually conditioned clearance on remedies. (As a DOJ trial attorney, I led the U.S. investigation, in cooperation with DG Comp staff.) Both agencies found that the combination raised competition concerns in the markets in specific sorts of data: "the distribution of aftermarket broker research reports, of earning estimates, of fundamental financial data of enterprises and of time series of economic data,"[7] to quote an EC press release. (The DOJ's Complaint omitted time series of economic data.)[8] For these specific types of data, Thomson and Reuters were leading providers in concentrated markets and there were good reasons to believe that other companies would not be able to enter to compete with them.

For example, one of the products at issue was fundamentals data. Thomson and Reuters offered years of fundamentals data for publicly traded companies around the world. In some countries, this data is relatively easy to obtain. In the United States, one can scrape SEC filings. In other countries, however, this was not the case, and entrants faced a significant barrier to entry. DOJ alleged:

> New entrants into the fundamentals data market, particularly with respect to international fundamentals data, must overcome significant barriers to entry. These include the difficulties of arranging for collection of data on tens of thousands of companies on a global basis, constructing a reliable historical database, the need to develop local expertise in each country's accounting norms, and the ability to develop data normalization and standardization processes. Therefore, entry or expansion by any other firm will not be timely, likely, or sufficient to defeat an anticompetitive price increase.[9]

DG Comp explained further. They emphasized the time and expense required for an entrant to offer global fundamentals data. "The hurdles come, first, from the need to collect fundamental data with a global coverage and second, to collect fundamental data going back in

[6] Wikipedia, *Craigslist Inc. v. 3Taps Inc.*, *available at* http://en.wikipedia.org/wiki/Craigslist_Inc._v._3Taps_Inc.

[7] European Commission, *Mergers: Commission clears acquisition of Reuters Subject to Conditions*, *available at* http://europa.eu/rapid/press-release_IP-08-260_en.htm.

[8] U.S. Department of Justice, Antitrust Division Decision of February 19, 2008, *available at* http://www.justice.gov/atr/cases/f230200/230281.htm.

[9] *Id.* at ¶37.

time several years."[10] In addition, significant work had to be done once data were collected. Vendors standardized data "by making accounts of companies reporting under different accounting rules comparable and responding to codification systems relevant to users."[11] "This also involves significant and particularly skilled manpower."[12] To carry out these processes "requires several years and significant investment and hence represents a huge barrier to entry."[13] But that may be the optimistic view, as DG Comp further explains that, according to market participants, "the raw materials needed to create these databases are simply unavailable at any price."[14]

The DOJ and DG Comp both undertook this sort of analysis separately for each of the data products as to which they brought a case. They did this because each of the products—while data—was different. The competitive dynamics at play in each market, while perhaps similar, were distinct. Also, of the scores of data products offered by Thomson and Reuters, most raised no competition concerns. As noted, DG Comp obtained commitments concerning only four products, and the DOJ's consent degree addressed three.

Maybe the Thomson/Reuters matter was unusual, particularly in that the data products at issue were sold to users as such. Would a different result apply where data are a key input to another product? Tucker & Wellford suggest so, arguing, "the notion of a relevant market consisting of internally used data is inconsistent with longstanding precedent that recognizes a market only where a product or service is sold to consumers."[15] But if internally used data are a key input rather than the product itself, surely a barrier to obtaining it can be a barrier to entry just the same. Suppose that Thomson and Reuters had not sold fundamentals data separately (as was Bloomberg's practice), but that it was an essential part of a terminal offering: While the relevant markets alleged by DOJ and DG Comp would have differed, the ultimate result would have been no different.

Manne & Sperry also question how market power fortified by data could be remedied. The Thomson and Reuters matter provides one answer, though surely not one which necessarily will fit other markets. In an agreement reached jointly with DOJ and DG Comp, Thomson and Reuters agreed to a form of remedy which would not have been possible with a non-digital good:

> [T]he parties committed to divest copies of the databases containing the content sets of such financial information products, together with relevant assets, personnel and customer base as appropriate to allow purchasers of the databases and assets to quickly establish themselves as a credible competitive force in the marketplace in competition with the merged entity, re-establishing the pre-merger rivalry in the respective fields.[16]

[10] DG Comp, *supra* note 7 at ¶361.
[11] *Id.* at ¶362.
[12] *Id.* at ¶363
[13] *Id.* at ¶364.
[14] *Id.* at ¶365
[15] Tucker & Wellford, *supra* note 2.
[16] DG Comp, *supra* note 7.

The combined Thomson Reuters continued to offer its predecessors' data products, but an entrant was enabled to go to market with a competing product based on a duplicate of the data. It is exactly the fact that data bases are not rivalrous that made this remedy possible.

Big data certainly can pose new and interesting problems for competition lawyers, but the notion that we categorically cannot identify barriers to entry or potential remedies in such product markets is not one of them.

CPI COMPETITION POLICY INTERNATIONAL

CPI Antitrust Chronicle
May 2015 (2)

No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals

Alec J. Burnside
Cadwalader, Wickersham & Taft LLP

www.competitionpolicyinternational.com

No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals

Alec J. Burnside[1]

I. INTRODUCTION

What is true of "free" lunches is true also of "free" search: there has to be a catch. By now it has dawned on most of us, as private individuals, how it is we are paying: not in cash, but in information about ourselves. The new dawn for the antitrust community needs to be the articulation of the consequences for antitrust analysis of this tectonic shift in business models.

The generational change in the leadership of the European Commission's antitrust work has coincided with a sudden spurt of attention to this topic—although it is perhaps no coincidence. In her confirmation hearing before the European Commission, Margrethe Vestager described personal data as "the new currency of the internet."[2] In this and other remarks she took up the themes launched into public debate by the European Data Protection Supervisor ("EDPS") in a discussion paper of March 2014 entitled *Privacy and Competitiveness in the Age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy.*[3]

The echo at the time from DG Competition was muted, but a conference seeking to breathe new life into the EDPS' unheard plea for debate in the antitrust community was held in February this year.[4] The keynote address was by Giovanni Buttarelli,[5] a privacy regulator

[1] Managing Partner at Cadwalader, Wickersham & Taft LLP, Brussels office.

[2] Commissioner-Designate Vestager, Hearing before the Committee on Economic and Monetary Affairs of the European Parliament (Oct. 2, 2014). Since taking office, Commissioner Vestager has reiterated these remarks: *see* Lewis Crofts & Robert McLeod, *In conversation with Europe's new Competition Commissioner*, MLEX, 5 (Jan. 1, 2015) ("Very few people realize that, if you tick the box, your information can be exchanged… you are paying a price, an extra price for the product that you are purchasing. You give away something that was valuable. I think that point is underestimated as a factor as to how competition works"); *see* Aoife White & Peter Levring, *EU Deal Probes May Weigh Value of Personal Data: Vestager*, BLOOMBERG BUSINESS (Apr. 9, 2015) ("Some companies, while apparently not generating euros or cents, still make money because holding very large volumes of data generates value").

[3] Preliminary Opinion of the European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy,* (Mar. 2014), *available* at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf.

[4] Concurrences and Cadwalader seminar, *Antitrust, Privacy & Big Data*, Brussels (Feb. 3, 2015). Synthesis *available at* http://www.concurrences.com/Photos/Antitrust-Privacy-Big-Data-1713/?lang=en.

[5] Mr. Buttarelli assumed office as the European Data Protection Supervisor in December 2014. The original paper was published in the term of his predecessor Peter Hustinx.

speaking to an audience drawn primarily from the antitrust circuit. My remarks on the day[6] sought to frame privacy and Big Data issues in the vernacular of antitrust. The growing interest in the topic is reflected in a number of conferences;[7] and for example, in a consultation on the "The commercial use of consumer data" launched by the U.K.'s Competition and Markets Authority in January 2015.[8]

The information collated by businesses about their customers evidently has an economic value justifying the cost of providing the service. The economics and business strategies around such datasets are not the focus of this contribution to CPI's colloquium. Instead the high-level conclusion, easily and quickly drawn, is that antitrust needs to evaluate the role and significance of datasets when they arise in the factual matrix of any assessment—be it dominance, restrictive practices, or merger review. Antitrust is not somehow set aside by the fact that a Big Dataset comprises information about individuals that may also be subject to privacy or data protection requirements.

Such an overlap in applicable rules is of course nothing remarkable in itself (consider LIBOR, where malpractice is the subject of both antitrust and financial services regulation[9]). But the question may fairly be posed as to the co-existence and interaction of these regimes.

II. "AS SUCH"

This issue has not been squarely presented in any decision of the EU Courts in Luxembourg, nor in the practice of the European Commission. The closest that the EU jurisprudence comes is a brief assertion in the *Asnef*[10] ruling of the Court of Justice. This was a case referred from the Spanish courts concerning a credit-worthiness register maintained among banks. The issue arising was one of information exchange among competitors—the information in question including personal data.

In framing the discussion the Court remarked that the "sensitivity of personal data" was not "as such" a matter for the antitrust laws. More fully it said: "…any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection."[11] The observation was

[6] Alec Burnside, *Setting the Scene* – Address at Concurrences and Cadwalader, Wickersham & Taft LLP seminar *Antitrust, Privacy & Big Data* (Feb. 3, 2015), *available at* http://www.concurrences.com/Photos/Antitrust-Privacy-Big-Data-1713/?lang=en.

[7] *See* e.g. *Briefing on Big Data, Privacy, and Antitrust* at George Mason University on March 18, 2015 (http://www.masonlec.org/events/event/288-briefing-big-data-privacy-antitrust), and the *17th International Conference on Competition* in Berlin on March 25-27, 2015 (http://ikk2015.de/Seiten/konferenzprogramm_e.html).

[8] The consultation is now closed and the CMA is reviewing public responses. Materials and feedback *available at* https://www.gov.uk/government/consultations/commercial-use-of-consumer-data.

[9] *See* Joaquin Almunia, *Statement on the euro interest rate derivatives case* (May 20, 2014), *available at* http://europa.eu/rapid/press-release_STATEMENT-14-166_en.htm.

[10] *See* Case C-235/08 Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios ("*Asnef*"), ECR I-11125 [2006].

[11] Case C-235/08 *Asnef* [2006], *Id.* at ¶ 63.

presented without greater discussion. Nor is the Advocate General's similar remark more expansive.[12] What then is the import and meaning of this statement?

It is hardly a blanket assertion that privacy is irrelevant to antitrust, or that antitrust must not address facts to which privacy laws may also be relevant. Rather, it indicates that antitrust rules should be applied in pursuit of antitrust goals. And indeed that is what the Court did in the case before it: apply the antitrust rules to a set of facts to which privacy disciplines had a parallel application.

The "as such" language, far from closing the door to the exercise of usual antitrust disciplines, in fact opens it. And the European Commission has passed through this open door, examining the economic relevance of control of large volumes of personal information.[13] It does so regardless of whether the individual-specific information in a dataset may also be governed by rules on privacy and the processing of personal data.

The relevance of antitrust goes beyond the obvious economic significance of Big Data (and of the sensitive personal information it comprises). It is not the goal of this contribution to multiply examples, but suffice it to note, for instance, that some service providers actively tout superior privacy characteristics as a quality differentiator.[14] Or note the commercial interests ranged against each other in the elaboration of a "Do Not Track" standard for internet searching.[15] It is a given that these matters must be debated in antitrust terms.

III. ANTITRUST (AND THE PURSUIT OF OTHER UNION OBJECTIVES)

It is, rather, the purpose of this contribution to fasten hard on the question whether (and how far) privacy considerations can be given weight within an antitrust assessment. That was not the topic before the Court in *Asnef*, where the comments were in any event (as English and U.S. lawyers might put it) *obiter*, i.e. an observation in passing which was not necessary for purposes of the immediate ruling.

Framing this very specific question invites echoes of older debates as to the application of competition policy to promote environmental or cultural objectives.[16] Citizens have an interest in clean air, but antitrust has never set itself up as a wholesale proxy for environmental policy. But it can give weight to environmental goals. So, for example, the Commission used its then power of exemption[17] to approve an otherwise restrictive agreement because it gave "direct practical effect to environmental objectives" defined in the directive on packaging waste.[18] Similarly it exempted

[12] *See* Opinion of Advocate General Geelhoed, Case C-235/08 *Asnef* [2006], ¶ 56:
"Any problems concerning the sensitivity of personal data can be resolved by other instruments, such as data protection legislation. It is clear that there must be some way of informing the borrowers concerned of what data are recorded and of granting them the right to check the data concerning them and to have them corrected where necessary. It appears that this point is settled, regard being had to the relevant Spanish legislation and also to clause 9 of the rules governing the register."

[13] *See* European Commission Decision 2014/C 417/02 (*Facebook/WhatsApp*), 2014 OJ C 417/4.

[14] For example, DuckDuckGo, *see* https://duckduckgo.com/—"the search engine that doesn't track you."

[15] *See* e.g. Fred B. Campbell Jr., *The Slow Death of 'Do NOT TRACK'*, N.Y. TIMES (Dec. 26, 2014).

[16] *See* JONATHAN FAULL & ALI NIKPAY, THE EU LAW OF COMPETITION 3.12 (6th ed. 2014).

[17] In the days before modernization under Reg 1/2003.

[18] *See* European Commission Decision 2001/837/EC (*DSD*), 2001 OJ L.391/1.

an agreement among appliance manufacturers to cease production of energy-inefficient machines identified by a directive.[19] In adopting this approach the Commission was giving due weight to the Treaty objective specifying the integration of environmental protection requirements into EU policies and actions.[20]

Similarly the Treaty calls for cultural aspects to be taken "into account in its action under other provisions of the Treaties."[21] DG Competition guidance on exemption under Art 101(3) recognizes that "goals pursued by other treaty provisions can be taken into account…".[22]

The examples cited above all concerned exemption criteria under Art 101(3), but a further example of cross-pollination, under Art 101(1), is provided by the Court of Justice in its *Allianz Hungaria* [23] ruling. Here the Court identified a restriction by object, drawing strength from an infringement of sectoral insurance rules. Domestic law required car dealers acting as insurance brokers to be independent from insurance companies, and to act in the best interests of policyholders. Arrangements (relating to the rate of payment for repair work to be done by the dealers) were, however, in place by which dealers were given conflicting economic incentives. The Court put weight on the breach of the insurance regulation in identifying a restriction of competition by object.

IV. APPLYING ANTITRUST (WITH PRIVACY IN MIND)

How then can antitrust align with and facilitate privacy goals? The superior norm is provided by the Charter of Fundamental Rights, which recognizes the protection of personal data as a specific right.[24] This right protects not only against interference by the state, but against any processing that does not meet minimum safeguards, i.e. processing "for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[25] In pursuit of this superior hierarchy requirement, and aligning with specific directives adopted to give effect to it, there is obvious scope for an application of the antitrust rules in a duly sensitive manner.

The EDPS has suggested, for example, that repeated breach of privacy rules may be an indication of abuse of a dominant position.[26] In this he was perhaps following a lead given by

[19] *See* European Commission Decision 2000/475/EC (*CECED*), 2000 OJ L 187/47.

[20] *See* Treaty on the Functioning of the European Union (TFEU), 2008 OJ C 115/53, art. 11.

[21] *Id.* art. 167(4).

[22] European Commission Guidelines on the application of Article [101(3) TFEU], 2004 OJ C 101/97, ¶ 42.

[23] Case C-32/11 Allianz Hungária Biztosító Zrt. and Others v Gazdasági Versenyhivatal ("*Allianz Hungaria*"), not yet reported [2013], ¶¶ 39-47.

[24] Charter of Fundamental Rights of the European Union, 2000 OJ C 364/10, art. 8

[25] *See* Preliminary Opinion of the European Data Protection Supervisor, *Privacy and competitiveness in the age of big data*, *supra* note 3, ¶ 16 et sub.

[26] European Data Protection Supervisor Giovanni Buttarelli, *Privacy and Competition in the Digital Economy* – Address at the European Parliament's Privacy Platform (Jan. 21, 2015), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-01-21_speech_GB_EN.pdf.

Commissioner Almunia who, as long ago as 2012, recognized that a "single dominant company could of course think to infringe privacy laws to gain an advantage over its competitors."[27]

The ability to retain customers despite serial disregard of their privacy interests might well be taken, first, as a confirmation of dominance, i.e. the ability to act without the need to be concerned about the reaction of competitors. And, secondly, the conduct could be thought of as exploitative abuse. In an old-economy mindset one would instinctively think of exploitation as extracting an excessive price.[28] But where the payment for the services received is not in cash but in personal data, the exploitation might perfectly well be found in the excessive harvesting of such data.

Such harvesting might be deemed exploitative where there is breach of legal privacy standards: the parallel to *Allianz Hungaria*[29] is a simple one. Data protection rules require unambiguous consent to the processing of personal data, and this principle is implemented in data protection rules, themselves the subject of reform and debate as to their adequacy. It is though plainly the reality that our data is being collated into datasets and used in ways beyond our knowledge or expectation: how many of us have ever consciously consented to receive targeted online advertising? Antitrust enforcement (pursued with a sensitivity to individuals' privacy interests) need not be aligned only on the breach of specific data protection rules. It can also be inspired directly from the higher Charter principle of minimum safeguards.

It will be argued against this that antitrust should not extend so far into another policy area; and doubtless more effective privacy regulation would reduce the reason for antitrust disciplines to be brought to bear. But this would hardly be the first occasion when EU antitrust enforcement has come to the aid of related policy areas, particularly where legislative reform has failed to advance. For a current example, consider the use of state aid disciplines to unlock the gridlock around unfair tax competition by EU Member States.[30] Similarly an activist antitrust enforcement policy served to secure passage of delayed legislation for the liberalization of the EU

[27] Joaquín Almunia, *Competition and personal data protection* – Speech at Privacy Platform event on Competition and Privacy in Markets of Data (Nov. 26, 2012), *available at* http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm.

[28] *See* Faull & Nikpay, *supra* note 16, at 4.16 et sub.

[29] Case C-32/11 *Allianz Hungaria* [2013], *supra* note 10.

[30] *See* e.g. Commission Press Release *State Aid: Commission extends information enquiry on tax rulings practice to all Member States*, IP/14/2747 (Dec. 17, 2014). The European Commission has opened investigations against tax rulings in Ireland (SA.38373 relating to Apple), Luxembourg (SA.38375 relating to Fiat Finance and Trade and SA.38944 relating to Amazon), the Netherlands (SA.38374 relating to Starbucks) and Belgium (SA.37667 relating to its excess profit tax system). DG Comp's commitment to the issue is also reflected in the introduction of the Task Force on Tax Planning Practices. This enforcement activity is to be seen against the background of legislative gridlock in the reform of corporate taxation. For that broader context see the Communication from the Commission to the European Parliament and the Council on *Tax transparency to fight tax evasion and avoidance*, COM(2015) 136 final (Mar. 18, 2015), *available at*: http://ec.europa.eu/taxation_customs/resources/documents/taxation/company_tax/transparency/com_2015_136_en.pdf.

energy market.[31] The pattern is an old one: as long ago as 1988 the competition rules were used to launch the process of telecoms liberalization.[32]

Alternatively, simply mining the text of Art 102 for possible application to "free" services, the Article refers to the imposition of "unfair trading conditions."[33] Users have *de facto* no choice but to sign up to the terms and conditions of online services, in order to be able to progress to the next screen. And then they may have no practical choice but to accept changes to terms and conditions, if they want to continue using a service in which they have invested their data. Network effects may also play, to keep a user within the ecosystem populated by other users. Degradation to original privacy terms will not provoke users to switch to another provider if there is no effective alternative.

Default settings (rarely altered in practice, no doubt) might desirably specify a high level of privacy protection, but a dominant company—or one that achieves dominance and then degrades its privacy policies—might more readily set defaults to the other extreme. The fairness of "trading conditions"—here the provision of the online service in return for extensive (and often unwitting) waiver of privacy rights—is explicitly a criterion within Art 102.

Companies compete to get consumers to give up their data. All companies in this line of business must have privacy terms, regardless of whether they choose to promote their policy as a quality differentiator. But dominant firms can afford to be more casual about users' privacy than others. There is no reason for antitrust regulators to treat this as beyond their reach.

V. (INTERIM) CONCLUSIONS

Privacy and Big Data present new permutations, but familiar antitrust disciplines can be applied to an economy where personal data rather than cash is the currency of payment. There is innovative scholarship in the area, focusing on the phenomenon of "free"[34] and the dimension of quality[35] as opposed to price. Antitrust lawyers, economists and regulators should avoid fixation on price as their key yardstick. It is not apt to measure what needs measuring in relation to "free" business models.

Cash is not king in these markets. Of course finance-driven markets are never far away: the personal information with which we pay for "free" services is monetized to attract advertising

---

[31] Faull & Nikpay, *supra* note 16, at 12.09 ("The adoption of the Third [Liberalization] Package provides a good example of the interplay between liberalization and competition policy").

[32] *See* European Commission Directive 88/301/EEC on competition in the markets in telecommunications terminal equipment, 1988 OJ L.131/73; *see* Faull & Nikpay, *supra* note 16, at 13.05 ("Many of the competition law cases brought by the Commission have related to market situations where abusive behaviour crosses over regulatory obligations, and EU competition law enforcement has played a prominent role in further pursuing the liberalization agenda").

[33] *See* TFEU, *supra* note 20, art. 102(a).

[34] *See* e.g. Michael S. Gal & Daniel L. Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement*, UC Berkeley Public Law Research Paper No. 259425 (Jan 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2529425.

[35] *See* e.g. Ariel Ezrachi & Maurice E. Stucke, *The Curious Case of Competition and Quality*, University of Tennessee Legal Studies Research Paper No. 256; Oxford Legal Studies Research paper No. 64/2014 (Oct. 1, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494656.

revenues. That takes us into two-sided markets, beyond the reach of this contribution. But antitrust techniques can be applied to both sides of the equation.

Conclusions at this stage are interim only in the sense that we lack a body of decided cases. But antitrust has much to contribute. Dominant players may outpace the privacy legislator, but antitrust enforcement may be fleeter of foot. The race of course is not between the enforcers, but rather a joint pursuit of the consumer interest.

CPI COMPETITION POLICY INTERNATIONAL

CPI Antitrust Chronicle

May 2015 (2)

Privacy Considerations In European Merger Control: A Square Peg For A Round Hole

Paul Gilbert & Richard Pepper
Cleary Gottlieb Steen & Hamilton LLP

www.competitionpolicyinternational.com

Privacy Considerations In European Merger Control: A Square Peg For A Round Hole

Paul Gilbert & Richard Pepper[1]

I. INTRODUCTION

It is now trite to observe the amount of data generated by modern society. Statistics abound about the data-rich environment created by technological advances and the digital economy:

> every couple of days, humanity now generates 5 exabytes of data; this roughly corresponds to the volume of data produced in the entire period between the dawn of time and 2003;[2]
>
> every day, we create 2.5 quintillion bytes of data—so much that 90% of the data in the world today has been created in the last two years alone.[3]

These data may be personal: social media content, eMail addresses, employment histories, financial information, shopping habits, and so on. Commercial enterprises (online and offline) proactively collect these types of data to improve their services, design and target marketing, and sell to third parties. This raises real questions about how to protect personal data against unauthorized or inappropriate use. The European institutions have recognized this challenge and are progressing towards a more stringent, harmonized data protection regime through the proposed General Data Protection Regulation.[4]

Several observers have also called for privacy to play a greater role in merger control, including under the European Merger Regulation.[5] Notably, in a 2014 preliminary opinion, the European Data Protection Supervisor criticized the European Commission for not assessing market power by reference to "control of commercialisable personal information" and instead adopting "a purely economic approach to the [*Google/DoubleClick*] case" where it failed to consider "how the merger could have affected the users whose data would be further processed by merging the two companies' datasets … that were not envisioned when the data were originally submitted." In doing so, the Commission was said to have "neglected the longer term impact on the welfare of millions of Users in the event that the combined undertaking's

---

[1] Paul Gilbert and Richard Pepper are, respectively, counsel and associate in the London and Brussels offices of Cleary Gottlieb Steen & Hamilton LLP. They are grateful for the assistance of Maurits Dolmans in preparing this article. The views expressed are personal and all errors are their own.

[2] Fabien Curto Millet, *La concurrence dans l'economie numerique*, A QUOI SERT LA CONCURRENCE 480 (2014).

[3] www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

[4] This paper does not address the debate over whether over-zealous privacy regulation may stifle innovation and create barriers to entry for small- and medium-sized enterprises, at a time the European Union is seeking to re-energize an entrepreneurial spirit in a digital single market.

[5] Council Regulation (EC) No 139/2004 of January 20, 2014 on the control of concentrations between undertakings.

information generated by search (Google) and browsing (DoubleClick) were later processed for incompatible purposes."[6]

This paper argues that privacy concerns should not enjoy specific privileges under the European Merger Regulation and there are no sound policy reasons that support their introduction. It observes the ways in which privacy issues are already taken into account in the Commission's substantive assessment, and it highlights the risks that arise from an over-emphasis on access to data in merger control.

II. PRIVACY CONCERNS DO NOT ENJOY SPECIFIC PRIVILEGES UNDER THE EUROPEAN MERGER REGULATION

Merger control in Europe developed with an explicit and exclusive focus on competition. As Nicholas Levy has described, "in the final negotiations during late 1988 and 1989 leading to the adoption of the Merger Regulation … the principal debate at the time was between those favouring a competition-based test and those urging that explicit account be taken of social, industrial, and employment considerations."[7]

That debate culminated in a purely competition-based substantive test: The Commission must prohibit mergers that would significantly impede effective competition and approve those that would not.[8] Neither the Commission's ability to take account of efficiencies[9] nor its power to accept commitments[10] undermines this principle; both require an assessment of competition in the relevant market.

The Commission has observed these principles in its decisional practice (as noted by the European Data Protection Supervisor in its 2014 preliminary opinion). Two cases, in particular, illustrate the point. First, in *Google/DoubleClick*, the Commission considered whether contractual restrictions on the use of data collected by DoubleClick might be jeopardized after it was integrated with Google. The Commission stressed that its decision "refers exclusively to the appraisal of this operation with Community rules on competition" and that the parties would remain subject to other legal obligations: "irrespective of the approval of the merger, the new entity is obliged in its day to day business to respect the fundamental rights recognised by all relevant instruments to its users, namely but not limited to privacy and data protection."[11]

---

[6] *Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Market*, Preliminary Opinion of the European Data Protection Supervisor, ¶¶ 62-66 (March 2014).

[7] Nicholas Levy, EUROPEAN MERGER CONTROL LAW: A GUIDE TO THE MERGER REGULATION ¶ 2.03 (2014).

[8] The 1989 Merger Regulation contained a test as to whether a concentration "creates or strengthens a dominant position as a result of which competition would be significantly impeded." This was recast in 2004 to consider whether a concentration would "significantly impede effective competition."

[9] Recital 29 of the European Merger Regulation notes it is "appropriate to take account of any substantiated and likely efficiencies" but makes clear that this consideration relates to the determination of the "impact of a concentration on competition in the common market."

[10] Recital 30 of the European Merger Regulation notes the Commission should be able to declare a concentration compatible with the common market where commitments are "proportionate to the competition problem and entirely eliminate it."

[11] Case COMP/M.4731 *Google/DoubleClick*, ¶¶ 258-265 and 368.

Second, in its 2014 review of the *Facebook/WhatsApp* merger, the Commission disregarded privacy issues upfront when assessing the impact of the transaction on the provision of advertising space and provision of user data valuable for advertising purposes:

> Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.[12]

III. POLICY REASONS DO NOT SUPPORT THE INTRODUCTION OF PRIVACY AS A DISCRETE CRITERION IN MERGER CONTROL

It is clear that privacy is not currently a discrete criterion for substantive assessment under the European Merger Regulation. This leaves the question of whether it should be. In the view of the authors, it should not.

The case for including privacy as a discrete consideration rests, presumably, on the concern that the merged firm might exploit data in ways that were not anticipated by individuals when they consented to their data being used by one of the merging parties. To illustrate, assume you provided information about your medical history to a life assurance company which is subsequently acquired by a bank. The bank may have an incentive to use your information in ways you had not anticipated, such as deciding whether to offer you a mortgage.

This may be a real concern, both at an individual level and for society as a whole. But that does not make it a question for merger control, any more than whether a merged firm should be allowed to make staff redundant or increase productivity in a way that may harm the environment (both of which might be viewed as efficiencies in a conventional merger control analysis).

Merger control seeks to protect the competitive process from structural market changes that threaten the efficient allocation of resources. This increases productivity, ensures continued innovation, and maximizes consumer welfare:

> effective competition brings benefits to consumers, such as low prices, high quality products, a wide selection of goods and services, and innovation. Through its control of mergers, the Commission prevents mergers that would be likely to deprive customers of these benefits by significantly increasing the market power of firms.[13]

In contrast, privacy legislation seeks to protect individuals (specifically their personal data) from unwarranted exploitation by commercial enterprises and governmental organizations. The European Court recognized this distinction in its 2006 *Asnef-Equifax* judgment: "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection."[14]

---

[12] Case COMP/M.7217 *Facebook/WhatsApp*, ¶ 164.

[13] Commission's Guidelines on the assessment of horizontal mergers (the "Horizontal Guidelines"), ¶ 8.

[14] Case C-238/05 *Asnef-Equifax v Ausbanc*, ¶ 63.

The focus of merger control on questions of competition does not undermine the importance of privacy law or any other issue that could be affected by market concentration. The issues are complementary. To the extent European stakeholders have concerns about the scope of data protection, there is no better case for using merger control to address them than for any other social agenda.

IV. PRIVACY ISSUES CAN BE RELEVANT TO THE SUBSTANTIVE ASSESSMENT OF MERGERS

None of this prevents the Commission from taking privacy issues into account in its substantive assessment under the European Merger Regulation. As consumers become more aware of privacy issues, both the ways firms manage and protect their data and the controls they offer to consumers are becoming important parameters of competition.[15] Firms offer robust protections and controls to protect personal data from inadvertent disclosure not only because they are required to do so by law, but because it strengthens their competitive offering.

The Commission highlighted data protection as a competitive differentiator between consumer communications applications in the *Facebook/WhatsApp* case: "These differences related to … (iv) the privacy policy (contrary to WhatsApp, Facebook Messenger enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities)."[16]

This is most obviously relevant when the Commission assesses a horizontal overlap between the merging firms to consider whether a concentration would "eliminate[e] important competitive constraints on one or more firms."[17] These constraints can include privacy policies as a qualitative aspect of the parties' offerings. Where a merged firm would have reduced incentives to promote or invest in privacy protection, that may be a relevant factor in the competitive assessment. This could apply even where the parties did not have access to large quantities of data. The removal of an important "maverick" that has developed innovative data-protection and control systems could potentially raise competition issues by reducing innovation in data privacy, even if the merging parties were not otherwise close competitors.[18]

Two points nevertheless bear emphasis. First, the Commission's role is to assess the effect of a merger on the competitive process. Privacy protection may be part of that dynamic but it is not its object. Second, we must guard against the creation of an "efficiency offence." If a merged firm can analyze data more effectively than the merging parties, this should improve the quality of their services and stimulate rivals to respond—which is all to the benefit of consumers.

---

[15] The European Data Protection Supervisor recognized this in the 2014 preliminary opinion: "In certain markets, consumers may consider a privacy-friendly service to be of better quality than a service which has an unclear or opaque privacy policy. In the provision of legal and medical services, private banking, security services, and exclusive luxury resorts, businesses typically compete on protecting privacy" (¶ 73).

[16] *Facebook/WhatsApp*, ¶102.

[17] Horizontal Guidelines, ¶ 22(a).

[18] The Horizontal Guidelines note: "in markets where innovation is an important competitive force … effective competition may be significantly impeded by a merger between two important innovators" (¶ 38).

V. INTERVENTION SHOULD BE THE EXCEPTION, NOT THE RULE

Indeed, competition authorities should be slow to intervene where competition drives firms to use data more effectively.[19] The Commission's decisional practice reflects this and a clear analytical framework has emerged.

First, there is a distinction between firms that use data as an input for their own services and those that sell data as a separate commercial activity. There is no economic market for the former. In *Facebook/WhatsApp*, for example, the Commission noted that neither party sold data to third parties and found no basis for defining a market for personal data.[20] Rather, the Commission defined a market for online advertising and analyzed the impact of the accumulation of user data by Facebook on that market. The Commission has reached a similar conclusion in several other cases.[21]

Second, where data are used solely as an input, the pertinent issue is whether access to those data acts as a barrier to entry. This is unlikely to be the case in many instances, for several reasons:

- **Data are cheap.**[22] As the Executive Office of the U.S. President has observed, "we live in a world of near-ubiquitous data collection" with "near-continuous collection, transfer, and re-purposing of information."[23] The costs of collecting, storing, and analyzing data are low and continue to decline with the costs of the relevant technology[24] as variable-cost cloud computing replaces fixed-cost proprietary infrastructure.
- **Data are non-rivalrous.**[25] Personal data collected by one firm are not used up—the same information is still available to others. An individual's age, for example, can be collected by a social media platform, an eMail provider, an eCommerce shop, or an off-line loyalty card program. The circumstance that one platform has collected a piece of information does not preclude another from doing the same.

---

[19] For a discussion of the European Commission and U.S. authorities' review of relevant competition cases, *see* Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, ANTITRUST SOURCE (2014).

[20] *Facebook/WhatsApp*: "The Commission has not investigated any possible market definition with respect to the provision of data or data analytics services, since, subject to paragraph (70) above, neither of the Parties is currently active in any such potential markets" (¶ 72).

[21] Cases COMP/M.4726 *Thomson/Reuters*; COMP/M.5529 *Oracle/Sun Microsystems*; COMP/M.5232 *WPP/TNS*; COMP/M.6314 *Telefónica UK/Vodafone UK/Everything Everywhere/JV*; COMP/M.6921 *IBM Italia/UBIS*.

[22] According to one observer, basic demographic information sells for about $0.0005 per person; even a detailed profile of an individual about to make a purchase—and therefore valuable to advertisers—typically costs well under one dollar. (*See* Emily Steel, *Financial Worth of Data Comes in at Under a Penny a Piece*, FINANCIAL TIMES (July 12, 2013).)

[23] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values 2* pp. 4 and 39 (2014).

[24] James Manyika, et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity,* MCKINSEY GLOBAL INST. (June 2011): "The ability to store, aggregate, and combine data and then use the results to perform deep analyses has become ever more accessible as trends such as Moore's Law in computing, its equivalent in digital storage, and cloud computing continue to lower costs and other technology barriers."

[25] The Commission recognized this in *Google/DoubleClick*: "the combination of data about searches with data about users' web surfing behaviour is already available to a number of Google's competitors today" (¶ 365).

- **Data ownership is dispersed.** The increasing digitization of products and processes has resulted in data being held by billions of individuals around the world. This makes it nearly impossible for any one player to foreclose its rivals.
- **Historic data have little value.** "70% of unstructured data is stale after only 90 days,"[26] so data collection and analysis increasingly occur on a real-time basis. Historic data collected by incumbent platforms provide little competitive advantage. There are many examples of new entrants disrupting markets and quickly acquiring leading positions, despite the presence of supposedly stronger incumbents.
- **Data are subject to diminishing returns.** While data can generate benefits, the marginal value of additional data for statistical analysis is limited. As explained by Fabien Curto Millet, a tenfold increase in data only divides the margin of error of a prediction by three.[27] Success comes from using personal data effectively, not from collecting every last item of available information. The key issue is processing and analysis; the scarcity is human talent.

The Commission has investigated whether access to data could operate as a barrier to entry on several occasions and never found this to be the case. In *Google/DoubleClick* the Commission found that merging the parties' data sets and data tools would not foreclose rivals: "Other companies active in online advertising have the ability to collect large amounts of more or less similar information that is potentially useful for advertisement targeting."[28]

In *Microsoft/Skype* the Commission found barriers to be low, citing the quick growth of Facebook and the "immediate success" of new entrants Viber, Fring, and Tango.[29] In *Facebook/WhatsApp* the European Commission found "there are currently a significant number of market participants that collect user data alongside Facebook" and that "there will continue to be a large amount of Internet user data that are valuable for advertising purposes and that are not within Facebook's exclusive control."[30]

All these decisions recognize that the collection and analysis of personal data are likely to be concerns only in the most exceptional of cases.

VI. CONCLUDING REMARKS

Privacy is not the objective of merger control, nor should it be. The objectives of competition law and privacy law are complementary and there is no sound basis for confusing the two. That does not prevent the Commission from analyzing the way firms compete to offer better protections and controls over personal data. But that is an analysis of the competitive process, not the adequacy of the privacy protections themselves.

---

[26] Citi Research 2013 Retail Technology Deep Dive.

[27] Millet, *supra* note 2.

[28] *Google/DoubleClick*, ¶¶ 269 and 364. The U.S. Federal Trade Commission reached the same conclusion. (*See* FTC Statement in *Google/DoubleClick*, FTC File No. 071-0170, page 12: "neither the data available to Google, nor the data available to DoubleClick, constitutes an essential input to a successful online advertising product.")

[29] Case COMP/M.6281 *Microsoft/Skype*, ¶¶ 90-93.

[30] *Facebook/WhatsApp*, ¶¶ 188-189.

The occasions when access to personal data results in barriers to entry or other competitive harm are likely to be rare, and the Commission's experience bears this out. By contrast, market solutions are certainly the best way of enhancing privacy protections for consumers beyond the minimum protections guaranteed by privacy law. Intervention in that competitive process should be the exception, and not the rule.

CPI COMPETITION POLICY INTERNATIONAL

CPI Antitrust Chronicle
May 2015 (2)

The Proper Role of Privacy in Merger Review

Darren S. Tucker
Morgan, Lewis & Bockius LLP

The Proper Role of Privacy in Merger Review

Darren S. Tucker[1]

I. INTRODUCTION

There have been increasing calls for the Federal Trade Commission ("FTC") and U.S. Department of Justice ("DOJ") to consider the potential loss of consumer privacy as a factor in their merger reviews and to challenge mergers of firms with large stores of personal data that otherwise pose no apparent competitive issues.[2] These calls are unlikely to be successful. Standalone privacy concerns cannot be factored into the merger review process in a way that is consistent with the antitrust statutes and existing precedent. There are also good policy reasons against incorporating traditional privacy concerns into antitrust doctrine.

Nevertheless, in industries where firms differentiate themselves through their approaches to privacy, a merger could reduce the incentive of a merged entity to compete on this basis. A substantial lessening of this competition could be a basis on which to block a proposed transaction. Still, the number of transactions that will raise serious concerns about loss of privacy competition is likely to be very limited even in digital markets.

II. IS PRIVACY A RELEVANT CONSIDERATION IN COMPETITION LAW?

There remain many unanswered questions about the scope of the Sherman and Clayton Acts, but whether these statutes reach consumer protection concerns such as privacy is not one of them. The U.S. Supreme Court has made clear on numerous occasions that non-competition factors cannot be considered in antitrust analysis. The Court has explained that antitrust law is concerned with fostering vigorous competition, on the view that this will lead not only to the lowest prices, but also to the highest quality products and the greatest degree of innovation.

As far back as 1931, the Supreme Court held that standalone consumer protection concerns may not be addressed using competition law.[3] In *FTC v. Raladam Co.*,[4] the Court held that a company's deceptive advertisements for an obesity cure were beyond the FTC's "unfair methods of competition" jurisdiction unless the FTC could show that there was a reduction in competition. This decision led Congress to pass the 1938 Wheeler-Lea Amendments to the FTC Act, which expanded the FTC's jurisdiction to include "unfair or deceptive acts or practices."[5]

In a series of subsequent decisions, the Court reaffirmed that competition is the lodestar of antitrust analysis and that courts may not consider other factors. For example, in *United States*

---

[1] Darren Tucker is a partner in the Washington, D.C. office of Morgan, Lewis & Bockius LLP.

[2] *See, e.g.*, Comments of the Electronic Privacy Information Center (EPIC) to FTC Remedy Study (Mar. 17, 2015), *available at* https://epic.org/privacy/internet/ftc/Merger-Remedy-3-17.pdf.

[3] For a history of privacy enforcement and its relationship with antitrust doctrine, *see* Maureen K. Ohlhausen & Alexander Okuliar, *Competition, Consumer Protection, and the Right (Approach) to Privacy*, 80 ANTITRUST L.J. __ (forthcoming 2015).

[4] 283 U.S. 643 (1931).

[5] Act of Mar. 21, 1938, ch. 49, § 3, Stat. 111 (codified at 15 U.S.C. § 45(a)).

v. Philadelphia National Bank,[6] the Court held that the effect upon competition is the sole criterion to determine whether a merger violates Section 7 and that consideration of other social or economic factors (there, the prospect of bringing more jobs to the merged entity's home city) was improper.[7]

Given the text of the antitrust statutes, no other result would be justified. Section 7 of the Clayton Act requires a showing that the effect of an "acquisition may be substantially to lessen competition," Sections 1 and 3 of the Sherman Act require a restraint of trade, and Section 2 of the Sherman Act requires an act of monopolization. These requirements, all of which reflect a goal of unfettered competition, do not lend themselves to the protection of interests such as privacy.

The antitrust agencies have likewise explained that antitrust law is only concerned with competitive effects. The 2010 Merger Guidelines state that the only consideration in merger analysis is whether a transaction "may substantially lessen competition."[8] The words "privacy" and "data protection" do not appear anywhere in the Guidelines. The FTC explicitly rejected calls to consider privacy in competition analysis in *Google/DoubleClick* and did so implicitly in *Facebook/WhatsApp* as well.[9]

This judicial and agency restraint rests on firm policy grounds. For one thing, privacy is difficult to quantify compared to traditional antitrust factors like price and output. How would one determine the effect on consumer welfare from a change in a company's privacy policy or data security practices? This concern is compounded by the variety of concepts of privacy. In addition, consumers have mixed views about the optimum level of privacy. Unlike lower prices, which can be observed and which consumers universally value, the concept of "more" or "better" privacy is not always clear and consumers value privacy in different ways, with some viewing it as a detriment.[10]

In a law enforcement system based on both antitrust and privacy considerations (or other non-competition considerations), there will be frequent tensions between the two modes of analysis. For example, aggregation of personal data from a corporate acquisition might raise concerns about greater privacy intrusions, but the antitrust laws would view this aspect of the

[6] 374 U.S. 321, 371 (1963) (holding that a merger that substantially reduces competition "is not saved because, on some ultimate reckoning of social or economic debits and credits, it may be deemed beneficial").

[7] *See also N.C. State Bd. of Dental Exam'rs v. FTC*, 135 S. Ct. 1101, 1109 (2015) (stating that the antitrust laws are intended "to promote robust competition;" lower court affirmed the FTC's rejection of non-competition defenses); *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 463 (1986) (health and safety defense asserted by dentists refusing to provide x-rays to insurance companies is "nothing less than a frontal assault on the basic policy of the Sherman Act"); *United States v. Nat'l Soc'y of Prof'l Eng'rs*, 435 U.S. 679, 690 (1978) (the rule of reason inquiry under the Sherman Act "is confined to a consideration of impact on competitive conditions").

[8] U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines § 1 (2010) [hereinafter Merger Guidelines], *available at* http://www.ftc.gov/os/2010/08/100819hmg.pdf.

[9] The European Court of Justice and European Commission likewise rejected calls to consider privacy in competition matters in *Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios (Ausbanc)* and *Facebook/WhatsApp*, respectively.

[10] Witness the millions of people that have public Facebook profiles and the many others who seek to maximize the number of followers on their Twitter or other social media sites.

combination as a potential efficiency due to the potential for lower costs and development of better services. Without a clear standard for how to weigh the competition versus the privacy considerations, the outcome is likely to reflect the personal views of the particular enforcer reviewing the transaction, ultimately leading to less predictability and less consistency in outcomes.

An additional concern is that competition remedies are not well suited to address privacy concerns. As the FTC pointed out in its *Google/DoubleClick* closing statement,[11] privacy enforcement through merger control may result in uneven privacy restrictions on market participants, which could have an adverse effect on competition. In particular, firms that are able to collect significant amounts of personal data unilaterally would have a competitive advantage against firms that seek to obtain similar data sets through acquisition. This might advantage large, vertically integrated incumbents against smaller rivals and new entrants.

Finally, it is unclear what shortcoming of consumer protection enforcement exists that would justify the need for expanding antitrust's reach. The FTC and state attorneys general have a long history of protecting consumer privacy through their consumer protection authority, and the Consumer Financial Protection Bureau has joined these efforts in the financial sector. These enforcers, supplemented by appropriate private enforcement, already have the necessary tools to address concerns about consumer harm from mistreatment of personal data.

III. IS PRIVACY A FORM OF NON-PRICE COMPETITION COGNIZABLE BY THE ANTITRUST LAWS?

In most industries, firms compete to sell their goods or services on the basis of price, features, and distribution, among other dimensions. In some markets, these other dimensions include competition on the basis of their privacy or data security protections.[12] A company may seek to gain users by advertising that it collects no personal information or that it encrypts communications with its users, for example. In theory, a merger between firms that are close competitors on the basis of their privacy protections could lead to anticompetitive effects, in much the same way that a merger between two firms that are close competitors on the basis of their product features could lead to anticompetitive effects.

In recognition of this, the antitrust agencies consider the potential loss of privacy competition in the course of their merger reviews. In the *Google/DoubleClick* investigation, the FTC considered whether the "transaction could adversely affect non-price attributes of competition, such as consumer privacy."[13] Several FTC officials have recently stated that the agency is paying attention to privacy competition in merger investigations. In addition, the 2010 Merger Guidelines place greater emphasis on the role of non-price competition.

Despite what appears to be a widespread recognition that privacy can be a form of non-price competition cognizable under the Merger Guidelines, there does not appear to be any

[11] Statement of Fed. Trade Comm'n at 2, *Google/DoubleClick*, FTC File No. 071-0170 (Dec. 20, 2007), *available at* http://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

[12] Although privacy and data security are distinct concepts, for simplicity I refer to both as "privacy" for the remainder of the article.

[13] *Google/DoubleClick* Statement, *supra* note 11, at 2-3.

generally accepted means of assessing which transactions will lead to anticompetitive effects due to a loss of privacy competition. This may be due in part to the lack of empirical evidence indicating that a larger firm would treat consumer privacy less favorably than a smaller firm. There is at least some (admittedly mixed) empirical evidence suggesting that higher concentration levels are correlated with higher prices. However, neither economic theory nor empirical evidence suggests a consistent relationship between industry concentration and the degree of privacy protection offered (or even product quality generally).[14]

To the extent there is a link between concentration and privacy, it may well be a positive relationship, i.e., larger firms may tend to protect privacy better than smaller firms. A firm that reduced its privacy protections to collect more data would be marginally adding to its costs for the purpose of delivering a better product—hardly the type of conduct we would expect from a firm with substantial market power.[15] In addition, larger firms are under greater scrutiny by the press, consumers, and regulators. Data breaches, changes in privacy policies, and enforcement actions against larger firms are widely reported in the press. In addition, larger firms have more resources to devote to data security and privacy.

Nevertheless, one could apply a standard Merger Guidelines unilateral effects analysis to evaluate the loss of privacy protection from a proposed merger or acquisition. Under this approach, potential concerns may arise when each of the following elements are met in addition to satisfying the standard structural case:[16]

- The merging firms are significant rivals due to their competition on privacy;
- A large share of customers regard the merging parties as offering the best products as a result of their approaches to privacy; and
- Rivals must be unlikely to revise their approach to privacy to better compete with the merged firm (i.e., no repositioning).

As part of the assessment of competitive effects, the reviewer would also consider other standard Merger Guideline factors such as entry, efficiencies, and the failing firm defense. A benefit to this approach is that there is no need to quantify the strength of a company's privacy offerings or determine the "optimum" level of privacy for consumers in the industry or even any particular segment of consumers. All that matters is that a substantial number of consumers view the merging parties as offering the best services specifically because of their privacy policies. When these conditions hold, the merged company will be able to successfully exercise market power because few of its customers will defect to other suppliers.

---

[14] OECD, *The Role and Measurement of Quality in Competition Analysis* 7 (2013) ("The empirical evidence that is available suggests that increasing competition can have either positive or negative effects on quality levels, depending on the particular market circumstances.").

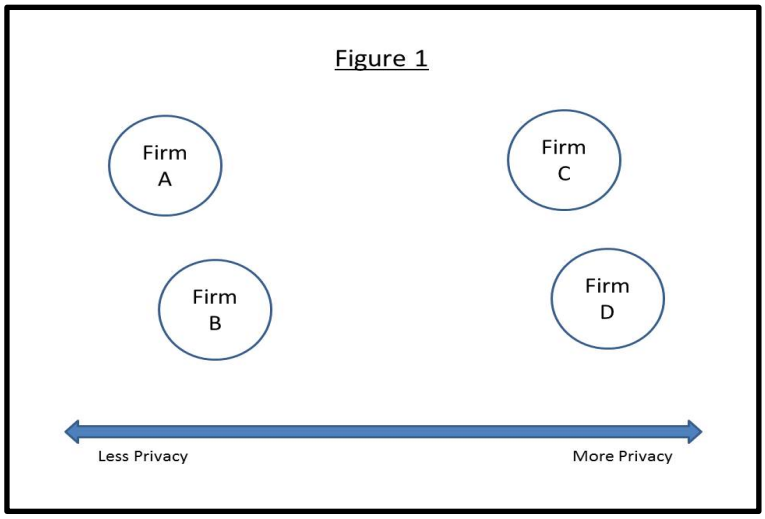
[15] James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1135-36 (2013).

[16] FTC Commissioner Julie Brill has proposed a similar inquiry. *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data 7 (June 2, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf.

Another benefit to this approach is that it will not condemn any transactions beyond the standard unilateral effects test in the Merger Guidelines. By employing a similar approach as Section 6.1 of the Merger Guidelines, the three-part test allows a reviewer to isolate the source of the unilateral effects as coming from privacy competition, as opposed to some other form of competition (e.g., product features, quality). The risk of Type 1 error, which is likely to be high when dealing with an abstract concept such as privacy competition, should accordingly be minimized.

One takeaway from this test is that even in a market where firms compete on the basis of privacy, unilateral effects are unlikely unless the merger is between two firms with strong privacy protections. Transactions such as *Facebook/WhatsApp*—where the concern was that Facebook might revise WhatsApp's more consumer-friendly privacy policy and apply Facebook's policy—are the least likely to raise unilateral effects concerns regarding loss of privacy competition. Instead, a merger between firms that both offer greater privacy protections than other market participants is far more likely to lead to anticompetitive privacy effects.

For example, assume Firms A, B, C, and D are competing social networks and that consumers select their provider based on a number of considerations. For some consumers, the decision of which provider to use is driven largely by the providers' privacy protections. Firms A and B offer relatively limited privacy protections, while Firms C and D offer greater privacy protections. As a result, Firms C and D attract many of their users due to their favorable privacy policies. This is illustrated in Figure 1.



If Firm A were to acquire Firm C, it is unlikely that Firm A would revise Firm C's approach to privacy to be less consumer friendly. If it did, many of Firm C's users would switch to Firm D, making the privacy change unprofitable.

In contrast, if Firms C and D were to merge, they could revise either or both of their approaches to privacy to be less consumer-friendly while losing little overall business.[17] So long as Firms C and D continue to offer better privacy protections than Firms A and B, few customers of Firms C and D will defect and a reduction in privacy will be profitable.

Notice that the strength of these results depends on how many of Firm C and D's customers selected those firms based on their privacy policies. The less significant the role of privacy in consumers' choice of providers, the less significant are the unilateral effects from a merger between Firms C and D because more users of C and D will be willing to switch to A or B.

Likewise, these results also depend on Firms C and D offering significantly better privacy protections than most other industry participants. If all four firms offered comparable privacy protections, many users of C and D's services would switch to A or B, making a diminution of privacy unprofitable.

In other words, unilateral privacy effects are only likely to arise where privacy is an important element of competition and the merger is between two firms that offer stronger privacy protections than most other rivals. These are necessary, but not sufficient, conditions for unilateral effects to arise. As noted above, a merger that satisfied the three-part test would pose no problems if there were *de novo* entry, significant merger-specific efficiencies, or other successful defenses.[18]

Another, potentially counterintuitive takeaway is that the injury to consumers from a loss of privacy competition is not necessarily less privacy. To be sure, a company acquiring a close competitor on the basis of privacy could exercise its newfound market power by reducing its privacy protections. But far more likely, it would simply increase prices or, in a market with zero prices, reduce investment in its services. According to FTC guidance, companies must take certain potentially unattractive steps before weakening their privacy policies,[19] whereas a price increase or reduction in investment could be implemented immediately and with no specific regulatory oversight.

In sum, privacy as an element of competition will be a relevant consideration in very few merger reviews, which may explain why no case has been brought along these lines. For the rare merger that presents a genuine risk of loss of privacy competition, the most likely harm to consumers would be fairly ordinary: higher prices or lower quality of services, not diminished privacy protections.

---

[17] Here I assume that the merging firms would have an incentive to reduce privacy protections to collect more user data, thereby generating greater revenue. As noted in the main text, there are reasons to question the accuracy of this assumption.

[18] As evidenced by the Facebook/WhatsApp transaction, consumers with strong privacy preferences may switch to upstart competitors in large numbers if there are concerns that a transaction will lead to a reduction in privacy. *See* Case COMP/M.7217—*Facebook/WhatsApp*, Comm'n Decision, ¶ 174 (Mar. 10, 2014) ("Privacy concerns also seem to have prompted a high number of German users to switch from WhatsApp to Threema in the 24 hours following the announcement of Facebook's acquisition of WhatsApp.").

[19] FTC Blog, *Mergers and Privacy Promises*, Mar. 25, 2015, https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.