DISSOLVING PRIVACY, ONE MERGER AT A TIME: COMPETITION, DATA, AND THIRD PARTY TRACKING

Reuben Binns* Elettra Bietti**

Amid growing concern about the use and abuse of personal data over the last decade, there is an emerging suggestion that regulators may need to turn their attention towards the concentrations of power deriving from large-scale data accumulation. No longer the preserve of data protection or privacy law, personal data is receiving attention within competition and antitrust law. Recent mergers and acquisitions between large digital technology platforms have raised important questions about how these different areas intersect and how they can complement one another in order to protect consumer welfare while ensuring competitive markets.

This paper draws attention to one particularly complicated kind of digital data-intensive industry: that of third party tracking, in which a firm does not (only or primarily) collect and process personal data of its own customers or users, but rather data from the users of other 'first party' services. Mergers and acquisitions between firms active in the third party tracking industry raise unique challenges for privacy and fundamental rights which are often missed in regulatory decisions and academic discussions of data and market concentration. In this paper, we combine empirical and normative insights to shed light on the role of competition regulators in addressing the specific challenges of mergers and acquisitions in the third party tracking industry. After critically assessing some of the US and EU case law in this area, we argue that a bolder approach is needed; one that engages in a pluralist analysis of economic and noneconomic concerns about concentrations of power and control over data.

CONTENTS

I. INTRODUCTION

Amid growing concern about the use and abuse of personal data over the last decade, there is an emerging suggestion that regulators may need to turn their attention towards the concentrations of power deriving from large-scale data accumulation. No longer the preserve of privacy and data protection law, personal data is receiving attention within competition and antitrust law, as illustrated by the German Bundeskartellamt's recent antitrust investigation into Facebook' user data practices.[1] Recent mergers and acquisitions between large digital technology platforms have raised important questions about how these different areas intersect and how they can complement one another in order to protect consumer welfare while ensuring competitive markets. The picture is complicated by the nature and structure of certain data-intensive markets, which are often multi-sided, fast-growing, characterized by network effects, and awash with venture capital which obscures long term business models in ways that defy short-term market definition. Digital markets give rise to "*an interesting atypical form of competition*,"[2] where companies simultaneously compete and collaborate, through a dynamic characterized by complex interlocking and conglomerate anticompetitive effects.[3]

This paper draws attention to a particularly obscure digital data-intensive industry; that of *third party tracking*, in which a firm does not (only or primarily) collect and

* Department of Computer Science, University of Oxford.
** Harvard Law School.
[1] Bundeskartellamt [BKA] [Federal Cartels Office] *Prohibition Decision: Facebook Inc. i.a. - The use of abusive business terms pursuant to Section 19 (1) GWB* (2 June 2019) (Germ.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568; Bundeskartellamt [BKA] [Federal Cartels Office] *Press Release Bundeskartellamt prohibits Facebook from combining user data from different sources* (February 7th, 2019), (Germ.), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.
[2] ARIEL EZRACHI AND MAURICE STUCKE, VIRTUAL COMPETITION, THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY 147 (2016).
[3] *Id*. at 147, *see* the notion of "frenemies".

process personal data of its own users, but rather the data of users of other 'first party' services. For instance, the online advertising network DoubleClick (recently re-branded by parent company Google as part of the 'Google Marketing Platform') provides ad serving and tracking technology which first party services can embed in their websites, which allows DoubleClick to profile users and target advertisements to them. The business models of third party tracking vary, but often include the profiling of users for targeted advertising and extracting insights from their behaviour for analytics. We focus on mergers and acquisitions of third-party tracking firms because they raise unique challenges which are often missed in regulatory decisions and academic discussions of data and market concentration.

Combining an empirical methodology with a critical assessment of some of the existing case law on these issues in the US and EU, we argue that a bolder approach to merger review is needed; one that engages in a pluralist analysis of economic and noneconomic concerns about concentrations of power and control over data. We show that the consumer welfare standard and the difficulties attached to measuring data-related harms have led to a failure to address the important harms resulting from data-heavy transactions.

Part II comprises a brief overview of the technical elements of third party tracking and of the business practices associated with it, and includes a discussion of some of the ways that antitrust authorities have been characterizing these activities.

Part III sets out the discussion on the relationship between competition and privacy. It presents two competing paradigmatic views of the role and scope of competition law enforcement: the purist neoclassical view, according to which the privacy impacts of mergers are not within the scope of the antitrust analysis, and the pluralist view, according to which a plurality of values including privacy inform antitrust analysis. Part III also develops an understanding of the pluralistic value of data as an asset in this context.

In support of the pluralist view, Part IV presents an analysis of consolidations amongst third party trackers on 5,000 of the most popular websites and mobile applications. We identified a subset of acquisitions between third party tracking firms which are most significant in terms of the data sources being merged as a result.

Relying on this dataset, Part V highlights why it may be important to consider the specific kinds and sources of first party data that each of the third parties involved in a consolidation has access to, for both competitive market and privacy reasons. In Part VI, we turn to analyzing the practice of the European Commission and the US Federal Trade Commission in relation to mergers in the third party tracking sector, assessing the extent to which these competition authorities' practices reflect on the significance of the data-mergers identified in Parts III and IV. We note three things. First, that only a proportion of cases which we consider significant are in fact reviewed by competition authorities. Second, that amongst the transactions that have in fact been scrutinized from a competition law perspective, only a small proportion are examined in depth. Third, after an analysis of this latter subset of decisions, we argue that competition authorities' approach largely focuses on first

party aspects, more or less consciously eliding the substantial third party tracking issues that arise. Further, many of the privacy harms at stake appear to have been ignored or consciously dismissed as irrelevant to a sound antitrust analysis.

Finally, Part VII concludes by summarizing and reflecting on some of the unique challenges raised by consolidation in third party tracking markets for regulators. The way these are addressed depends on evolving institutional views about the relationship between competition and data protection. We thus argue in favor of a pluralist approach, to inform a collaborative dialogue between competition and data protection authorities.

**

II. AN OVERVIEW OF THIRD PARTY TRACKING

This section provides an overview of what third party tracking is, and how antitrust and competition authorities have addressed it, if at all, in reviews of transactions between firms that engage in third party tracking.

2.1 Third party tracking technology

We use 'tracking' here to denote a range of data collection and processing practices which aim to collate the behaviours and attributes of end-users of digital technologies. It is commonly used to refer to technology which is embedded by a *third party* on multiple *first party* websites or mobile applications.[4] Third parties create 'libraries' and 'software development kits' for mobile apps, or snippets of javascript code which can be embedded in the html source of a website page. Typically, when a user installs the app, or views the website, the third party code collects data from the session and associates it with a (usually unique) identifier, which is sent to a remote server controlled by the third party. Since the same third party code is typically embedded on multiple different websites or apps, a single user's behaviour on multiple different apps / websites can be combined into a single behavioural profile, which might include interests, demographics, content they viewed, or their geolocation data.[5]

---

[4] For definitions and empirical studies of tracking on the web and mobile, see e.g.: Gunes Acar et al., *The web never forgets: Persistent tracking mechanisms in the wild*, in PROCEEDINGS OF THE 2014 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 674 (November 2014); Zhonghao Yu et al., *Tracking the trackers*, in PROCEEDINGS OF THE 25TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 121 (April, 2016); Reuben Binns et al., *Third Party Tracking in the Mobile Ecosystem*, in PROCEEDINGS OF THE 10TH ACM CONFERENCE ON WEB SCIENCE 23 (May 2018), https://perma.cc/2J2J-XST3.

[5] For a comparison of the inclusion of third party code and libraries between web and mobile apps, see: Christophe Leung, Jingjing Ren, David Choffnes, and Christo Wilson. 2016. *Should You Use the App for That? Comparing the Privacy Implications of App-and Web-based Online Services.* In PROCEEDINGS OF THE 16TH ACM INTERNET MEASUREMENT CONFERENCE*;*

Third party tracking serves many different purposes. In some cases, it provides basic measurements for the first party, such as how an app or website is used, which pages are visited or when an error occurs. 'Audience measurement' and analytics services like Adobe Audience Manager go a little further, by matching website visitors to external information comprising their demographics and interests, and providing it back to the first party.[6] Others provide varieties of functionality such as payment provision, authentication or security, and track users across services for these purposes. For instance, Distil Network's 'Are You a Human' service tracks users across multiple sites, monitoring their behaviour to distinguish human users from the automated activity of software agents or 'bots' (a kind of automated Turing test).[7] This information is provided back to the first parties to help them automatically block bots from parts of the website or app. In many cases, third party tracking firms re-purpose the same tracking data for multiple different services; data ostensibly collected for analytics might later be used for targeted advertising or security.

Where the purpose is targeted advertising by marketers, behaviours that a user engages in on one website or app could feed into a profile which may lead to targeted advertisements being delivered on another website or app. For instance, viewing a pair of shoes on a fashion app or website might lead to the user seeing advertisements for the same product on a different app or website. Advertisers may pay the ad network per impression (i.e. the advert being displayed) or only if the user clicks, and the app developer / website owner will receive a portion of these revenues accrued by the ad network. While the provision of user data to ad networks is usually coupled with in-app or in-site display advertising, this is not always the case. In some cases, a third party might remunerate a developer / website owner for providing the data directly, rather than indirectly through targeted ad placements. While such firms are often vague about who their customers are, the data they buy may end up being sold to ad networks in order to target ads to users when they use other apps which *do* run display advertising.

In many cases, third party trackers do not provide monetary benefits to first parties, but instead provide some useful free service - such as analytics, proprietary fonts, or social media sharing buttons - and use these integrations as a means to collect user data for some other commercial purpose. For instance, Google Analytics provides a free service to website operators to understand how their users use the website, but such user data can also be re-used for targeted advertising purposes via other Google services like Google Ads.[8] Third parties like DoubleClick (also

---

Reuben Binns, Jun Zhao, Max Van Kleek, and Nigel Shadbolt., *Measuring third party tracker power across web and mobile*, 18 ACM TRANSACTIONS ON INTERNET TECHNOLOGY (September 2018).

[6] Adobe Audience Manager: https://perma.cc/7XXG-BGSZ

[7] Distil Networks: 'Are You A Human?' https://resources.distilnetworks.com/all-blog-posts/distil-acquires-are-you-a-human

[8] www.analytics.google.com/analytics

owned by Google / Alphabet), on the other hand, offer ad serving capabilities as a service.

The third party advertising technology ecosystem has evolved to encompass even more complex arrangements between multiple third parties. Some third parties specialize in matching online users to their offline profiles held by data brokers (e.g. LiveRamp, formerly a subsidiary of the data broker Axciom). The placement of advertisements often works through automated 'real time bidding' auctions, where software agents automatically bid on behalf of multiple advertisers for advertising opportunities in real time through an 'ad exchange' intermediary. The amount that advertisers are willing to pay will depend on what kind of users the first party can serve ads to; and the more that the first and/or third party knows about those users, the more they can charge the advertiser for the targeted advertising opportunity. Multiple ad networks might be embedded on the same app or website, allowing the first party to select whichever network offers the best remuneration for any given available space. In such cases, rather than integrating multiple different ad networks' code into a single app or site, many developers rely on ad network aggregators which handle multiple different networks and find the most profitable ads to serve in real-time.

Recent studies of third party tracking on the web and mobile apps show that tracking is almost ubiquitous, and most first parties include code which allows their users to be tracked by multiple third parties.[9] The kinds of data collected by third parties varies between devices, platforms, genre of app / website, and purpose of tracking.[10] At a minimum, third parties assign and / or record a unique identifier which allows an interaction to be associated with the user. Web browser information, such as the version number, plugins installed, and fonts used, is also often captured as it is often uniquely identifying in combination. Common kinds of data collected via smartphone applications include location data (which can be highly accurate using GPS), a list of other applications installed, the type of handset, etc. Beyond this, a range of information pertinent to the application and the purposes of tracking might be collected.

2.2 Competition authorities' assessment of third party tracking markets

The opacity and (often) lack of direct monetization of third party tracking activities has made them a much neglected aspect of digital markets for competition authorities. Competition authorities have tended to focus on specific purposes of third party tracking that constitute distinct markets, such as marketing information services or the sale of online advertising, rather than on the versatile third party tracking activities themselves, such as data collection, the training of complex machine learning models or the compilation of digital profiles. Authorities have focused on money flows rather than data flows, and on individuals as direct paying customers, rather than as remote third parties affected by a company's tracking activities while having no contractual relationship with the company itself.

[9] *Supra* note 4. .
[10] *Supra* note 5.

Under EU law, a "market" "*comprises all those products and/or services which are regarded as interchangeable or substitutable by the consumer by reason of the products' characteristics, their prices and their intended use"*.[11] In other words, a market constitutes a sector of activity characterized by a set of uniform characteristics which apply to all firms active in it, and which makes these firms' respective actions in that particular sector of activity interdependent. In light of their focus on money flows, the European Commission has been distinguishing at least two separate sectors of activity with broad overlaps with third party tracking: online advertising activities and data analytics services.

Regarding data analytics services, in *VNU / AC NIELSEN*[12] and *TELEFONICA / CAIXABANK*,[13] the Commission broadly distinguished the following categories: market research services, that consist of reports on consumer attitudes and actual purchasing patterns; marketing information services, that entail the creation and supply of data profiles on individual consumers for direct marketing purposes; and media measurement services, which are aimed at measuring the audience of specific media, such as television and internet. In this and other decisions concerning data analytics activities, the Commission focused on the sale or licensing of data, without investigating the upstream activities that are inputs to data analytics, which often entail data collection through third party tracking.

Regarding the online advertising market, the European Commission has been somewhat more specific. In its decision to clear the *Google/DoubleClick* merger in 2008,[14] the European Commission provided an overview of the functioning of online advertising services markets, determining that online and offline advertising services constituted two separate markets,[15] and exploring further segmentations of online markets, including the distinction between search and non-search online advertising,[16] and that between direct and intermediated sales of online advertising. In a similar fashion to the US Federal Trade Commission (FTC) in its decision on the same merger,[17] the Commission distinguished a number of possible forms of online advertising "intermediation". There are broadly three categories of

[11] European Commission Notice on the Definition of Relevant Market for the Purposes of Community Competition Law, at para 7, 1997 O.J. (C 372) 7, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31997Y1209(01).
[12] European Commission decision of 12 February 2001 in Case COMP M.2291 - VNU / ACNielsen, http://ec.europa.eu/competition/mergers/cases/decisions/m2291_en.pdf.
[13] European Commission decision of 14 August 2013 in Case COMP M.6956 - TELEFONICA/ CAIXABANK/BANCO SANTANDER/JV, http://ec.europa.eu/competition/mergers/cases/decisions/m6956_235_2.pdf.
[14] European Commission decision of 11 March 2008 in Case COMP M.4731 – Google / DoubleClick, http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf.
[15] This was for several reasons, including: the capacity of online advertising of being targeted at users; its capacity to let advertisers to know at a very high level of precision how many users have viewed or clicked on an ad; and also that pricing mechanisms are very different for online and offline advertising.
[16] European Commission in Google / DoubleClick, *supra* note 14, at 56.
[17] Statement of the Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170 (December 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

intermediaries: "ad networks," "ad exchanges" and "media agencies."[18] Ad networks are aggregators of online advertising space and act as a "single buying point" for advertisers.[19] Ad exchanges are instead auctions or marketplaces where advertisers and publishers can virtually meet and directly buy or sell ad space in real-time.[20] Finally media agencies buy aggregated advertising space for advertisers, who are their direct customers. Media agencies also operate through ad networks and ad exchanges. In addition, the Commission and the FTC both considered the market for ad serving tools, on which DoubleClick was active, which includes tools for generating, displaying, serving and measuring the reach of ads,[21] an activity closely associated with third party tracking.

In 2008, the EU Commission highlighted a trend towards vertical integration of intermediaries with ad serving providers.[22] While in some cases it attempted to distinguish between 'online' (more specifically, web-based) and mobile advertising,[23] advertising on PCs and mobile phones,[24] the EU Commission does not appear to have ever analyzed specifically whether tracking may be different on mobile or on the web.

Overall, the focus of competition authorities on "markets" as economically relevant sectors of activity has led to a focus on areas where data is sold for a direct profit such as data analytics services and the sale of advertising space and to their neglect of important challenges relating to the market power of certain entities whose third party tracking activities include indirectly monetized data collection, sharing and profiling.

One notable exception is the German Bundeskartellamt's *Facebook* investigation, where the authority has dwelled on third party tracking activities in a new way.[25] In the investigation, the German authority found Facebook dominant with a market share of daily active users of 95% in Germany.[26] Facebook was found to

---

[18] European Commission in Google / DoubleClick, *supra* note 14, at 20.
[19] *Id. supra*.
[20] *Id.*, at 21.
[21] *Id.*, section 6.1.3., and *see* Federal Trade Commission in Google / DoubleClick, *supra* note 17.
[22] European Commission in Google / DoubleClick, *supra* note 14, at 32.
[23] European Commission decision of 6 February 2013 in Case COMP M.6314 - Telefónica UK / Vodafone UK / Everything Everywhere / JV, e.g. at 5(3).
[24] European Commission decision of 3 October 2014 in Case COMP M.7217 – Facebook / WhatsApp., at 69.
[25] *See* Bundeskartellamt [BKA] [Federal Cartels Office] *Prohibition Decision: Facebook Inc. i.a. - The use of abusive business terms pursuant to Section 19 (1) GWB*
(2 June 2019) (Germ.),
https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568; Bundeskartellamt [BKA] [Federal Cartels Office] *Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*
(15 February 2019) (Germ.),
https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3; Bundeskartellamt [BKA] [Federal Cartels Office] *Background information of the Facebook proceeding* (February 7th, 2019),
https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6..
[26] Bundeskartellamt [BKA] [Federal Cartels Office] *Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*

abuse its dominant position by exploitatively conditioning access to and use of its platform on the combination of user and device-related data collected both directly on its site and on other third party sites which can be linked to the user's Facebook profile, e.g. through Facebook's APIs.[27] In its decision, the authority considered European data protection law as a standard for finding abusive behavior: in this case consent could not be said to be voluntary and freely given under the GDPR[28] because "*users consent to Facebook's terms and conditions for the sole purpose of concluding the contract*."[29] In the absence of other bases for lawful processing, Facebook's processing was found to violate data protection law. The Bundeskartellamt then considered whether such violation was evidence of an abuse of dominance. German law requires a showing that dominance and the violation of data protection rules are causally related.[30] This causal relation was present for two reasons. First, consent cannot be considered voluntary and freely given if users have no other choices. If Facebook had adequate competitors, there might have been valid consent. Second, those contracts allowed Facebook to access, collect and benefit from larger amounts of data than its competitors and arguably larger amounts of data than its users would agree to.

The German authority's novel approach to the relationship between competition and data protection law has raised suspicion amongst those who doubt the ability of an antitrust authority to effectively address privacy-related matters. Reasons for suspicion include: that the decision conflates two fields of enquiry; that it highlights questions that competition law is unequipped to address, or leads to jurisdictional complexities that would be better addressed through a different route. [31] In addition, as expressed by Justus Haucap, "*there is little evidence that would suggest that larger firms violate data protection and privacy standards in a more systematic fashion than smaller firms – if at all, the contrary appears to be true*."[32] This may be too quick a conclusion, however. As discussed in more detail below, large

(15 February 2019) (Germ.), pp. 3-7, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3,

[27] Abuses of dominance are unlawful under Article 102 of the TFEU, Consolidated Version of the Treaty on the Functioning of the European Union art. 102, May 9, 2008, 2008 O.J. (C 155) [hereinafter TFEU].

[28] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, O. J. L 119/1 (**GDPR**), Articles 6 and 7, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en.

[29] *Id. supra*, at 10.

[30] *Id. supra*, at 11.

[31] *See* e.g. Jakob Kucharczyk, *The German FCO's Facebook Case: Blurring The Line Between Competition And Data Protection Enforcement*, DISRUPTIVE COMPETITION PROJECT, February 8, 2019, http://www.project-disco.org/european-union/020819-german-fcos-facebook-case-competition-and-data-protection-enforcement/; Giuseppe Colangelo and Mariateresa Maggiolino, *Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S.* 8 INTERNATIONAL DATA PRIVACY LAW 224 (2018); Geoffrey Manne, *Doing double damage: The German competition authority's Facebook decision manages to undermine both antitrust and data protection law*, TRUSTONTHEMARKET BLOG, February 8th, 2019, https://perma.cc/D4XS-YURS

.

[32] Professor Justus Haucap, *The Facebook Decision: First Thoughts*, D'KART ANTITRUST BLOG, February 7th, 2019, https://www.d-kart.de/en/the-facebook-decision-first-thoughts-by-haucap/.

companies with greater tracking capabilities can access, process and control more information and thus may have a greater responsibility to comply with data protection laws.[33] In a recent paper, Ariel Ezrachi and Viktoria Robertson suggest that a detailed theory of harm that links data harvested through third party tracking to a degradation of consumer welfare is necessary, possibly because loose reliance on the notion of "*exploitative business terms*" is insufficient. [34]

Aside from the Bundeskartellamt *Facebook* decision – whose importance remains confined, for now, to Germany – the importance and impact of third party tracking does not appear to have been considered as such in competition authority merger decisions. As noted above, in both of their decisions regarding the *Google/DoubleClick* merger, the European Commission and the FTC refer to "third party ad serving" as the tools which enable the delivery and tracking of online advertisements, a market on which, at the time of the merger, DoubleClick was an active and predominant player.[35] The FTC dwells on some of the data aspects of ad serving technology, while maintaining a focus on its instrumentality to the sale of advertising space: *"Advertiser side ad servers also provide key data that is used to plan, manage, maintain, track, and analyze the results of online campaigns across multiple publisher websites. Like publishers, advertisers pay for the use of ad serving services on a cost per thousand ads served."*[36]

The role of third party data collection has also been ignored in merger decisions where the entities operate as both first and third parties. For example, in *Microsoft/LinkedIn*,[37] as discussed below, the European Commission analysed some of the merger's data aspects. However, it described Microsoft and LinkedIn's relevant datasets narrowly, including only the data collected from their respective customers, not the data these companies collect as third parties on other sites or apps: *"LinkedIn full data refers to all the data that LinkedIn collects, or could collect, and store about* ***its users and their activity****, such as professional details, connections, interests, posts, endorsements."*[38]

'*Users*' is unfortunately ambiguous. On a narrow interpretation, '*users*' might refer only to users of the main LinkedIn or Microsoft services (e.g. LinkedIn's professional social network, and Microsoft's search, email, and other software services). But on a broader interpretation, it might refer also to users of other

[33] *See* Orla Lynskey, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 Theoretical Inquiries in Law 189 (2019).
[34] Ariel Ezrachi & Viktoria H.S.E. Robertson, *Competition, Market Power and Third-Party Tracking*, 42 WORLD COMPETITION 5 (2019).
[35] European Commission, *supra* note 14; and *see* Federal Trade Commission in Google/DoubleClick, supra note 17.
[36] Federal Trade Commission, *supra* note 17, at 6.
[37] European Commission Decision of 6 December 2016 in Case M.8124 – Microsoft / LinkedIn, http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.
[38] *Id. supra*, at 12. Also see para 34: *"[T]he Transaction does not raise competition concerns resulting from the possible post-merger combination of the "data" (essentially consisting of personal information, such as information about an individual's job, career history and professional connections, and/or her or his email or other contacts, search behaviour etc.* ***about the users of their services****) held by each of the Parties in relation to online advertising.*" (Emphasis added.)

unrelated first party sites or apps on which their third party tracking services are embedded (such as Microsoft's Bing Ads and LinkedIn's Audience Network). This ambiguity elides the extent to which both firms were capable of tracking individuals outside of the Microsoft and Linkedin services, which could not have been properly considered without further large-scale investigation. As we argue below, these definitions illustrate an endemic propensity to focus on first party activities and to overlook third party tracking. By contrast, data protection authorities are increasingly alert to the need to protect such non-users, as illustrated in an ongoing case brought by the Belgian Privacy Commission (now the Belgian Data Protection Authority) in 2015 against Facebook for the large-scale tracking of internet users via third party tracking on websites even if they do not have an account with the social network.[39] We may, nonetheless, be witnessing a recent shift in competition authorities' willingness to expand their scope of enquiry in light of the Bundeskartellamt's *Facebook decision*[40] and of initiatives such as the EU Digital Clearinghouse[41] and the FTC's Hearings on *Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century*.[42]

**

III. COMPETING VIEWS OF ANTITRUST LAW AND OF THE RELATIONSHIP BETWEEN ANTITRUST AND PRIVACY PROTECTION

Before turning to our empirical findings and to the assessment of competition law merger decisions in the third party tracking industry, this section articulates some current debates underpinning the relationship of antitrust and privacy protection. While a first view sees competition law as a purist discipline whose goal is to ensure the efficiency of markets and the maximization of a narrow understanding of welfare and competitiveness mostly based on price, our preferred view is a pluralistic one, which sees competition law as one tool in a larger toolbox, enabling the promotion of a variety of economic values and societal goals. We then show that data has both economic and personal aspects, and argue that, without amounting to a pure commodity, data has market effects which can and should be considered by competition authorities.

6.1 The purist and pluralist views

The purist view

[39] *See* Belgian DPA, Press Release, *The Data Protection Authority defends its arguments before the Court of Appeal in Brussels in the Facebook case*, https://perma.cc/E6JL-U8CR.
[40] Bundeskartellamt [BKA] [Federal Cartels Office] *Prohibition Decision: Facebook Inc. i.a. - The use of abusive business terms pursuant to Section 19 (1) GWB* (2 June 2019) (Germ.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568
[41] *See* https://perma.cc/BUG4-NWKL.
[42] *See* the FTC's website at: https://perma.cc/GBV4-WMYD.

We define the purist conception of antitrust as the understanding that antitrust is a pure discipline with rigid boundaries, focused on the promotion of market efficiencies and the limited correction of market failures. The claim that underlies a purist view of antitrust law is that markets are mostly capable of correcting themselves and thus that any regulatory interference in markets must be kept to an absolute minimum.

Having first emerged in the 1940s, these so-called "neoclassical" economic ideas became part of President Regan's policies in the 1970s and 80s, and particularly influential in antitrust enforcement circles. They are characterised by: near blind faith in the efficiency of markets and in the uncoordinated choices of rational profit-maximizing economic actors; the idea that competition is a "*self-initiating process*"[43] that requires minimal regulatory intervention; and that "*the proper lens for viewing antitrust problems is price theory.*"[44] In Robert Bork's foundational work *The Antitrust Paradox*, he asserted that "*the only legitimate goal of antitrust is the maximization of consumer welfare,*"[45] and that "[i]*n judging consumer welfare, productive efficiency, the single most important factor contributing to that welfare, must be given due weight along with allocative efficiency.*"[46]

The tendency to confine the scope of antitrust law to narrow questions of market failure corrections, efficiencies and welfare narrowly conceived is perhaps most prevalent in the US, but can be noticed also in the decisions of European competition authorities. As demonstrated later in this paper, the attempt to maintain rigid boundaries for antitrust has indeed led EU and US regulators alike to overlook important concerns and to exercise bad judgment on whether certain data sensitive M&A transactions should be allowed to go through. Yet finding a unique and uncontroversial objective for antitrust regulation, or coming to a unified view on the meaning of consumer welfare, economic efficiency, economic freedom or an effective competitive process, is in our view practically impossible. Further, the attempt to confine the discipline's scope of application has led to a decline in the relevance of antitrust merger reviews in recent years. As Maurice Stucke has warned, maintaining a purist approach to antitrust law divorces the discipline from reality and risks rendering it obsolete.[47]

The pluralist view

Reliance on the Chicago School paradigm as the most promising model for disciplinary purity does not appear to have adequately equipped US antitrust authorities to address the needs of the digital economy: the DOJ brought thirty nine civil and three criminal monopolization cases between 1970 and 1972 and only one

---

[43] Unilateral Conduct Working Group, Report on the Objectives of Unilateral Conduct Laws, Assessment of Dominance/Substantial Market Power, and State-Created Monopolies (Moscow: International Competition Network, May 2007), http://www.internationalcompetitionnetwork.org/uploads/library/doc353.pdf.
[44] Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 UNIVERSITY OF PENNSYLVANIA L. REV. 925, 932 (1978).
[45] ROBERT H. BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF (1978), at 7.
[46] *Id. supra*, at 405.
[47] *See* Maurice Stucke, *Reconsidering Antitrust's Goals*, 53 BOSTON COLLEGE LAW REVIEW 551, 611 (2012), https://lawdigitalcommons.bc.edu/bclr/vol53/iss2/4.

since 2000.[48] Further, in the United States criticism is mounting against the neoclassical belief that monopolies that maintain low prices or offer free services increase consumer welfare;[49] if regulators fail to intervene, in the long run predatory pricing eliminates competitors allowing monopolists to charge higher prices and diminish consumer welfare. The focus on short term efficiencies to the detriment of long-term effects has begun to appear myopic.

But the flaws of neoclassical economic thinking are not the only reason to reject a purist perspective on competition law. Orla Lynskey has argued that traditional economic understandings of market power based on the ability to charge higher prices, as per the definition of market power in the EU *Horizontal Merger Guidelines*,[50] are too limited.[51] Economists unsurprisingly disagree on how to measure and understand market power from a purist economic perspective.[52] Lynskey's suggestion of a broader understanding of platforms' power that accounts for the non-economic values at stake in antitrust investigations that takes the distributional implications of power concentrations over data seriously is thus to be welcomed.[53] The pluralist perspective therefore urges thinking across and beyond competition and data protection's disciplinary boundaries, looking for solutions to the dynamically evolving digital sector.

6.2 The value of data

Data can be valued in different ways and for different purposes. Claims over data indeed can be understood in at least two distinct ways: (a) as claims based on proprietary or economic interests over data as an asset, including intellectual property rights or rights to use the data as part of an economic activity,[54] or (b) as claims based on personal human interests in data or dataflows as related to the shaping of one's own person and personal image in the eyes of others.[55] Both types of claims over data can exist simultaneously: a content sharing platform might have an economic interest in maintaining list of user names, their sex and their content preferences in order to better target ads at them and generate a profit; a user, on the other hand, might have a personal interest in the information that the platform holds about her. The platform or the community at large might also have other non-economic interests in the data: for instance, maintaining such a record of users or

[48] Maurice Stucke, *Should We Be Concerned About Data-opolies?* 2 GEO. L. TECH. REV. 275, 280 (2018).
[49] See e.g. Lina Kahn, *Amazon's Antitrust Paradox*, 126 YALE LAW JOURNAL 710 (2017).
[50] Council Regulation on the control of concentrations between undertakings (hereafter "Horizontal Merger Guidelines"), 2004 O.J. (C 31), at para 8.
[51] Orla Lynskey*, Regulating "Platform Power,"* LSE LAW, SOCIETY AND ECONOMY WORKING PAPERS (2017), http://www.ssrn.com/abstract=2921021 (last visited Aug 15, 2018).
[52] *See* the case of *Streetmap.eu Ltd v. Google Inc. & Ors* [2016] EWHC 253 (Ch), at para. 47, where the judge discusses contrasting economic experts' evidence.
[53] Also *see* Orla Lynskey, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 THEORETICAL INQUIRIES IN LAW 189 (2019).
[54] *See* eg. Jeffrey Ritter; Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L & TECHNOLOGY REV 220 (2018).
[55] *See* eg. MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE ENDS OF LAW (2015); HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF (2012).

individuals can be said to improve user-experience or lead to other societal gains that are independent of whether it allows the platform to generate a profit. To complicate the matter further, while an individual platform user may have personal interests over the data, other non-users of the platform might also have personal interests in that same data or data that has been opaquely linked to it. These various types of interests over data sometimes go hand in hand, and other times do not: for example when a user does not want the platform to hold information about them and use it for commercial purposes, or when a user accepts the platform's practices but a non-user is indirectly also affected by the practice and cannot object.

When it comes to the assessment of mergers in the third party tracking industry, considering data's value as both an economic asset and an individual or collective good could complicate competition authorities' task. Should they consider all data in terms of market effects? Should they refrain from considering these questions altogether and defer to data protection or other regulators? While acknowledging the difficulties underlying these questions, it must be recognized that it would be wrong for competition authorities to consider all data as pure economic assets and to subsume all data matters within routine competition law analysis. Although the parallels between information and money are striking,[56] data cannot be simply reduced to monetary value. As recent research has suggested, the value that we attach to digital goods is highly contextual and subject to variations, such as the so-called "*superendowment effect*," that are not explainable in mainstream economic terms.[57] On the other hand, a pluralist perspective on the role of competition law enforcement would allow competition authorities to construe questions of "market effect" or "market power" broadly enough to encompass the analysis of direct and indirect harms resulting from the creation of large concentrations of power and control over data. Considering data as being more like money, as some economists would be tempted to suggest, does not in our view solve the current problems that underlie mergers and acquisitions in the third party tracking industry. What would address the problem, is a bolder, more informed, consideration of the harms at stake, and of how individuals, be they users or third parties, are affected.

**

IV. EMPIRICAL INVESTIGATION OF DATA-COMBINATION RESULTING FROM THIRD PARTY TRACKER CONSOLIDATION

Third party trackers have commercial advantages over first parties; not only do they create efficiencies of scale by developing and maintaining tracking software, they can also aggregate data from multiple first party services to produce richer profiles of individuals. This is because they can access a richer pool of data and

[56] *See* e.g. Evgeny Morozov, *Digital Socialism? The Calculation Debate in the Age of Big Data*, NEW LEFT REVIEW (Mar-June 2019), https://newleftreview.org/issues/II116/articles/evgeny-morozov-digital-socialism, which critically explores the much glossed-over parallels between data and money.

[57] Angela G. Winegar, Cass Sunstein, *How Much Is Data Privacy Worth? A Preliminary Investigation*, JOURNAL OF CONSUMER PRIVACY (forthcoming, 2019).

may perceive themselves (perhaps incorrectly) to be less constrained by the need to directly engage with data subjects through privacy policies which might otherwise limit their data processing activities. By contrast, a first party website or app only has access to the data of its own users as they engage with that particular service. This makes the data less valuable as less is known about any given user. The reach of a third party tracker is important whether its purpose is ad targeting, analytics, or otherwise. Even the value of a security-oriented service like the bot-detection tracker discussed above is a function of its distribution across multiple first parties, because its bot-detection algorithm will be more accurate with more behavioural data on more users (and bots) from a variety of sources. Whatever its purpose, the extent to which a third party tracker is integrated into a large number of first parties, and the popularity of those third parties with users, is one of the key factors determining its power and potential profitability.

In previous work, these aspects of third party tracker power have been discussed in terms of *prevalence* – defined as the number of first parties on which a third party tracker is present – and *prominence* – where such prevalence is weighted by the number of users of the first parties.[58] Prevalence and prominence are both important; a tracker with high prevalence has the opportunity to combine user data from multiple different first parties, but if those first parties have very few users (i.e. low combined prominence) the data is likely to be less valuable. Conversely, a third party tracker which is present on a single very popular first party service will not have significantly more value than the first party itself; as such, it would have little value as an ad network, because advertisers or data brokers could deal directly with the first party instead.

A small number of companies dominate across both the web and mobile; these include technologies that are owned by Google (or its parent, Alphabet), Facebook, Twitter, Adobe, and others. Binns et al. used measures of prevalence and prominence, for web and mobile (both separately and combined), in combination with standard indexes of market concentration (e.g. the Herfindhal Hirschman Index) to measure the extent of concentration amongst third party trackers.[59] While these measures do not account for the *type* and *sensitivity* of data collected, they do provide a standardized and practical way of measuring the 'reach' of a given tracker. Such measures are useful if we want to understand the significance of a merger or acquisition involving one or more third party trackers, from the perspective of the data being combined and the power this brings.

This section presents an analysis of mergers and acquisitions involving third party trackers that are most significant in terms of the quantity and quality of data being combined. We use data from previous studies as a starting point, combined with external data on mergers and acquisitions, to identify the most significant data combinations resulting from transactions. We begin by describing the process of

[58] Steven Englehardt & Arvind Narayanan, *Online tracking: A 1-million-site measurement and analysis*, in PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 1388 (October 2016). .

[59] Reuben Binns, Jun Zhao, Max Van Kleek, and Nigel Shadbolt., *Measuring third party tracker power across web and mobile*, 18 ACM TRANSACTIONS ON INTERNET TECHNOLOGY (September 2018).

sampling, identifying, and calculating the prevalence and prominence of third party trackers on the web and mobile platforms, undertaken in previous research.[60]

3.1 Methodology

The data collection and analysis consisted of several steps:

1. **Selecting first party websites and apps:** First, a sample of the most popular websites and mobile applications were identified. For the web, this was based on the 5,000 most visited websites according to the global Alexa rankings.[61] For mobile applications, this was based on the 5,000 most popular applications listed in the U.S. and U.K Google Play Store (where popularity is measured by number of downloads).[62]

2. **Detecting third party trackers:** web trackers were identified using the OpenWPM web crawling tool, developed by researchers at Princeton,[63] which detects the presence of third party trackers through analysis of network traffic, generated during automated browsing sessions of the 5,000 websites. Mobile trackers were identified by downloading the 5,000 most popular Android applications, and applying an automated code analysis tool to detect the presence of third party code which included references to external host domains. Further details of methods for detection of third party trackers in both platforms can be found in the original paper detailing how the dataset was obtained and analyzed.[64]

3. **Collating company information, corporate relationships, and consolidations**: Having traced code libraries and domains associated to specific companies, we also compiled supplementary information about all of these companies' primary business, and whether it had any parent / subsidiary relationships with other companies. In the latter cases, we identified whether these relationships were the result of mergers and acquisitions, and if so, when those consolidations occurred. These were compiled from public sources including public registers of company ownership,[65] and the technology industry monitoring site like CrunchBase.[66]

---

[60] *Id. supra*.
[61] *See* Alexa.com.
[62] The choice of U.S. and U.K. app stores reflects the geographic scope of the study (U.S. and Europe). For data on the prevalence of trackers from different geographic regions, see id 46, section4.4 p6. We were unable to perform this analysis on the Apple iPhone app store due to various technical and legal restrictions prohibiting external analysis.
[63] *See* Steven Englehardt & Arvind Narayanan, *Online tracking: A 1-million-site measurement and analysis*, in PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 1388 (October 2016)..
[64] For details, *see* Reuben Binns et al., *Measuring third party tracker power across web and mobile*, 18 ACM TRANSACTIONS ON INTERNET TECHNOLOGY (November 2018), section 5.
[65] *See* www.opencorporates.com.
[66] *See* www.crunchbase.com.

4. **Measuring prevalence and prominence of third party trackers**: We then measured the *prevalence*[67] and *prominence*[68] of third party trackers on the 5,000 most popular websites and (Android) mobile apps. The third party tracking firm with the highest prevalence and prominence among first-party services, across both web and mobile, is the Alphabet group, which includes the most prevalent of all subsidiaries firms, the analytics service Google Analytics. The following table (**Table A**) lists the main trackers on web and mobile with their respective market shares (prevalence).

Table A: Top 3 third party trackers on web and mobile.

	Web[69]		**Mobile[70]**	
1	Google/Alphabet	70%	Google/Alphabet	88.44%
2	Facebook	40%	Facebook	42.55%
3	Twitter	25%	Twitter	33.88%

5. **Modeling the data-combination effect of each consolidation**: We then identified all the first party sites or apps from which data could be combined as a result of each merger or acquisition between two distinct third party trackers into a single tracker. To clarify, we are considering the potential for data collected by third parties embedded on first party services to be combined via those third parties if they consolidate (e.g. the consolidation of the advertising networks Criteo and DataPop); we are not considering the potential of data combination resulting from direct consolidations between first parties (e.g. where the music streaming service Lala.com was bought by Apple in 2009). We present two measurements which capture different aspects of the resulting data power of the merged entity:

    a. *Post-consolidation prevalence*: Prevalence is defined as the number of sites or apps on which a third party tracker is present in our datasets of the top 5,000 websites and Android apps. The prevalence of a consolidated entity will be the sum of the prevalence of each of the merged entities, minus any overlaps (i.e. first party sites on which both trackers were already present).
    b. *Post-consolidation new data combinations*: In some cases, two sources of first party data may have never previously been combined; a consolidation between two trackers may allow the combination of data from users of sites which was previously not possible due to the sites having no tracker networks in common. To measure the extent to which consolidations potentially result in such

[67] This is the number of first parties on which a third party tracker is present.
[68] This is prevalence weighted by the number of users of the first parties.
[69] *See* Joel Purra and Niklas Carlsson, *Third-Party Tracking on the Web: A Swedish Perspective* IEEE 41st CONFERENCE ON LOCAL COMPUTER NETWORKS 28 (2016).
[70] *See* Reuben Binns et al., *Third Party Tracking in the Mobile Ecosystem*, in PROCEEDINGS OF THE 10TH ACM CONFERENCE ON WEB SCIENCE 23 (May 2018).

new combinations of first party data, we counted the number of first party sites which did not already have both of the third party trackers embedded on them prior to the consolidation. See **Figure 1** below for an example.

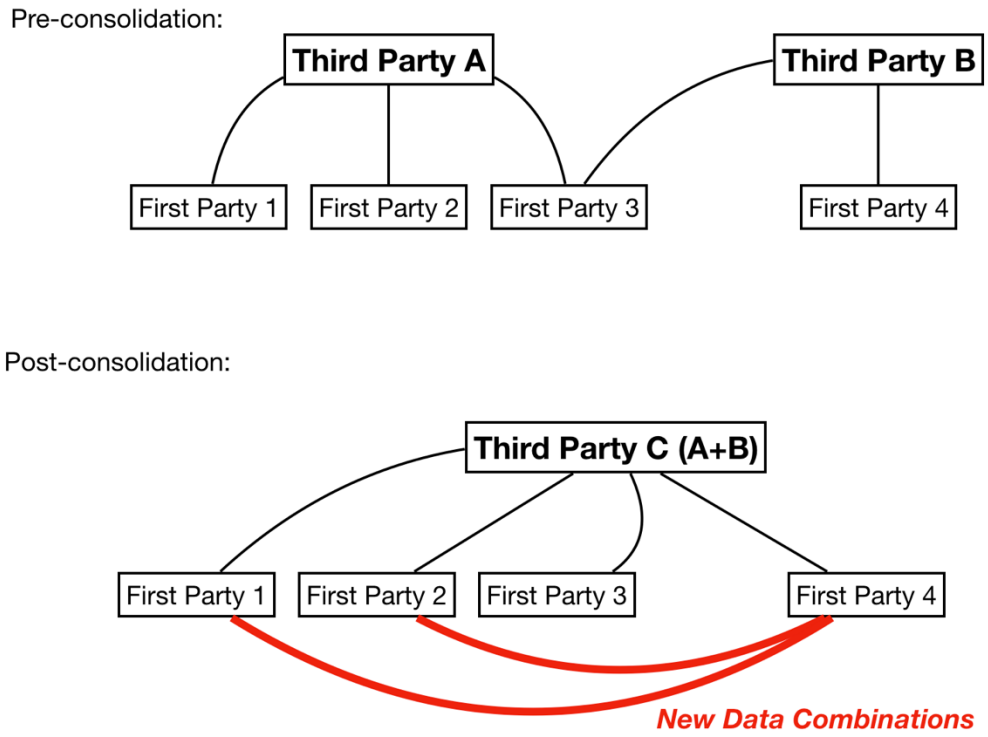

Figure 1 *If third party A is embedded on first parties (websites or apps) 1, 2, and 3, and third party B is embedded on first parties 3 and 4, then when A and B consolidate into new entity C, data from 1 and 2 is newly combined in a tracking network with 4 for the first time, whereas 3 and 4 were already combined via B.*

It is important to note some limitations of this method; the data represents the distribution of third parties on websites and apps at a single point in time (the data collection period spanned over November 2016-January 2017). Ideally, we would measure the prominence of the parties involved immediately prior to the acquisition, to get the most accurate picture of each party's reach at that point in time. But in practice, acquisitions and mergers occurred before and after the data collection period and in the intervening time the picture may have changed. For instance, we cannot know how the distribution of e.g. DoubleClick might have differed in the time between 2008 and 2018, if it hadn't been acquired by Google. Thus, when we discuss the data-combination associated with *Google / DoubleClick*, it is on the basis of the current distributions of the third party technology associated with each firm (which likely differed at the time of acquisition in 2008). However, unlike the *Google / DoubleClick* case, the majority of the transactions in question occurred within 2 years of the time of data collection. Another limitation is that we focus on samples of first parties (5,000 websites and 5,000 Android apps), rather than the entire web or Android app store or a smaller subset of the most popular websites; different samples would likely result in (small) changes in the significance of each consolidation. Finally, these calculations

assume that a consolidation does indeed result in data being combined in the resulting consolidated entity.[71]

(**TableB**) shows acquisitions between third party tracking firms. They are ranked in order of the number of new first party data sources which could be combined as a result of the consolidation. It also shows the prevalence for the parent firm after consolidation (the rank order for prominence is omitted for brevity, but similar). The 42 transactions in **Table B** represent the most significant combinations of first party data resulting from third party consolidation. We did not include transactions that involved less than 5 first party websites / mobile apps (0.001% of the apps / sites in the sample), or acquisitions of a company active in third party tracking by a company which itself had no prior significant third party presence.

[71] We acknowledge that not every consolidation will necessarily result in data-merging, However, the majority do, often despite promises to maintain separation between data sources, which may later be broken or circumvented, as in the case of *Facebook / WhatsApp*, *supra* note 24.

Table B: New 1st party combinations, Prevalence per transaction

	Year	Target	Acquirer	New 1st Party Combinations	Prevalence
1.	2006	**Youtube**	**Google**	8293	77.3
2.	2014	**Firebase**	**Google**	8262	77.3
3.	2009	**Admob**	**Google**	7233	77.3
4.	2012	**Instagram**	**Facebook**	5111	39.25
5.	2007	**DoubleClick**	**Google**	4872	77.3
6.	2014	**Liverail**	**Facebook**	4745	39.25
7.	2013	**Mopub**	**Twitter**	3956	15.45
8.	2013	**Crashlytics**	**Twitter**	3661	15.45
9.	2017	**Yahoo**	**Verizon**	2133	0.055
10.	2016	**Linkedin**	**Microsoft**	1654	16
11.	2014	**Bitstadium**	**Microsoft**	1615	14
12.	2014	**Flurry**	**Verizon**	1014	0.055
13.	2015	**Appnexus**	**Yieldex**	939	0
14.	2014	**Bluekai**	**Oracle**	769	0.7
15.	2017	**Moat**	**Oracle**	767	0.7
16.	2015	**Maxymiser**	**Oracle**	766	5.7
17.	2016	**Addthis**	**Oracle**	766	0.7
18.	2015	**Datapop**	**Criteo**	632	6
19.	2014	**Adquantic**	**Criteo**	632	6
20.	2014	**Tedemis**	**Criteo**	632	6
21.	2014	**Adcolony**	**Opera**	500	0.05
22.	2013	**Umeng**	**Alibaba**	290	1.48
23.	2014	**Rocketfuel**	**Xplus Two**	206	0
24.	2016	**Flashtalking**	**Encore Media Metrics**	172	0

25.	2017	**Intowow**	**Verizon**	5	0.055
26.	2011	**Sizmek**	**Vector Capital**	2	0
27.	2016	**Tube Mogul**	**Adobe Systems**	0	5.7
28.	2016	**Livefyre**	**Adobe Systems**	0	5.7
29.	2011	**Typekit**	**Adobe Systems**	0	5.7
30.	2018	**aerserv**	**inmobi**	0	1
31.	2017	**Flickr**	**Verizon**	0	0.055
32.	2017	**Tumblr**	**Verizon**	0	0.055
33.	2017	**Millenialmedia**	**Verizon**	0	0.055
34.	2016	**krux**	**salesforce**	0	0.2
35.	2017	**Brightroll**	**Verizon**	0	0.055
36.	2017	**One By Aol**	**Verizon**	0	0.055
37.	2017	**Gravity Insights**	**Verizon**	0	0.055
38.	2010	**Admarvel**	**Opera**	0	0
39.	2017	**Aol**	**Verizon**	0	0.055
40.	2011	**Demdex**	**Adobe Systems**	0	4.5
41.	2017	**Radium One**	**RhythmOne**	0	0.8
42.	2016	**Tapad**	**Telenor**	0	0

**

V. THE PRIVACY AND COMPETITION ASPECTS OF FIRST PARTY DATA COMBINATIONS RESULTING FROM THIRD PARTY MERGERS

Before turning to an analysis of antitrust decision-making in this sector, in this section we illustrate why the nature of the first party data being combined by third parties is important, by picking a few instances from the dataset discussed above. Combinations of specific kinds of data into one post-merger entity can raise two sorts of concerns: (1) privacy concerns arising from the merger of different

databases; and (2) questions related to the combined entity's resulting commercial advantage vis-à-vis its competitors, customers or suppliers.

First, the particular combinations of first party data are important from a privacy perspective, because if the acquisition results in user data from two different services being merged into a single user profile, new privacy risks may arise. Pre-acquisition, an individual might have a profile at company A which contains their browsing habits on news websites, and another profile at company B which contains their medical search history from health websites. Post-acquisition, these profiles from A and B may be merged into a single profile linking information contained in both. Now, the individual's news media interests can be correlated with their health condition; their medical searches might feed into a targeted advertisement that appears when they read the news. The 'new first party combinations' column of **Table B** quantifies the extent to which consolidations could have resulted in such new combinations of first party data.

Take, for example, Adobe's acquisition of Tubemogul in 2016. Tubemogul is an ad network which tracks the activity of visitors to various websites, including the health website MensHealth.com; after acquisition by Adobe, such data would likely have been integrated into the profiles contained in Adobe's existing ad technology platform which is present on 10% of the most popular websites, including many of the largest news, travel and retail services. For users of the health website, a significant change will have occurred in terms of the richness and sensitivity of the data contained within those profiles. They may find that the symptoms they entered into a health website could be combined with the political news articles they read, resulting in the possibility of their being targeted as a democrat-voting diabetic, for example, which would not have been possible without that particular acquisition.

Second, specific combinations of data sources might significantly determine a combined entity's post-merger commercial opportunities, such as its market position, market power and ability to access neighboring markets, as well as the kinds of services it can provide and the value of the data it holds post-transaction. An ad network which is prevalent on social networks, might significantly increase the value of its targeting by acquiring a target which is prevalent on dating apps, if the value of social network data to ad targeting in the context of dating is high (or vice-versa). Similar combinations were involved in the case of AOL's acquisition of Flurry; Flurry tracks 5 million users through the social network app TimeHop, which was combined with AOL's existing tracking technology embedded on dating apps like TopFace and Queep (10 million users each). Likewise, the ability to identify visitors to a property search website might be much more valuable if one also has the ability to identify the same users in a finance app in which people are likely to click on mortgage adverts. This may be the case for Krux, present on property search site iScout (5 million users), which was acquired by Salesforce which is present on the German finance advice site Finanzen.net. Such examples suggest that the kinds of sites a third party tracker has access to - whether in terms of the kinds of user data it has access to, or ability to place ads - may determine the kinds of advertising clients they attract and the value of their services. This type of combination can have important effects on market competition.

Interestingly, consideration of the different types of data collected by the merging entities and consequences for post-merger competitiveness were in fact raised in the European *Google/DoubleClick* merger decision. The Commission noted that the types of data that would be combined as a result of the merger could potentially impact competition:

> Competition based on the quality of collected data … is not only decided by virtue of the sheer size of the respective databases, but also determined by the different types of data the competitors have access to and the question which type eventually will prove to be the most useful for internet advertising purposes.[72]

However, the way that different kinds of data from first and third party services might interact was not discussed in this case.

This section has shown that competition and data protection considerations are much more entangled than one could initially have envisaged in relation to mergers and acquisitions. The next section extends this argument, by examining competition authorities' approach in greater depth. As we will see, competition authorities have largely glossed over questions of how the types of data being merged can contribute to privacy intrusions or to an increase in control and economic power. Further data aspects have rarely if ever been addressed head on by any of the authorities whose decisions we examined.

**

VI. COMPETITION LAW ANALYSIS OF DATA-SIGNIFICANT TRANSACTIONS

After identifying the 42 relevant M&A transactions through the approach described in Part IV, we then searched for each transaction in the databases of five competition authorities, to determine whether the transactions have been scrutinized from a competition law perspective:[73] the US Federal Trade Commission,[74] the European Commission,[75] the UK Consumer Markets Authority (CMA),[76] the French antitrust authority[77] and the Italian Autorità Garante della Concorrenza e del Mercato (AGCM).[78]

[72] European Commission, *supra* note 14, at para. 273 and 360.
[73] Note that the choice of these five competition authorities was based on the authors' resources, linguistic abilities and experience navigating the authorities' sites. While we left out the German Bundeskartellamt, we are mindful that this authority's activity should be scrutinized in future work on competition law and third party tracking.
[74] Federal Trade Commission site: https://www.ftc.gov/enforcement/merger-review.
[75] European Commission DG Competition site: http://ec.europa.eu/competition/elojade/isef/index.cfm?fuseaction=dsp_merger_ongoing.
[76] UK Competition and Markets Authority site: https://www.gov.uk/cma-cases.
[77] French Autorité de la Concurrence: http://www.autoritedelaconcurrence.fr/user/tableaudcc.php.
[78] Italian Autorità Garante della Concorrenza e del Mercato: http://www.agcm.it/en/search.html.

We noted that out of the 42 transactions, only 21 were scrutinized by one or more of the five competition authorities which we focused on (see **Table C** below). We found no decisions by the French and Italian authorities, in spite of one of the companies at stake, Criteo, being French. We found one decision by the UK CMA's predecessor, the Office of Fair Trading. Most of the decisions we found were summary clearances, and only five of the 42 transactions were the subject of in-depth competition law investigations by one or more of these authorities: seven full-merits decisions in total.[79] In only four of these seven decisions, competition/antitrust authorities actually explored the overlaps of competition and data protection law when it comes to the merger of different entities' datasets, and in all four they appear to dismiss those issues.[80]

For thoroughness, we also checked the databases to see if any of the companies involved in those mergers were also involved in other transactions which were reviewed in depth by these five competition authorities in spite of not leading to an actual merger. We found one such transaction: Microsoft's acquisition of Yahoo Search. The European Commission and the US Federal Trade Commission cleared

[79] European Commission decision of 11 March 2008 in Case COMP M.4731 – Google / DoubleClick, http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf, Statement of the Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170 (December 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf, Statement of the Federal Trade Commission Concerning Google/AdMob, FTC File No. 101-0031 (May 21, 2010), https://www.ftc.gov/sites/default/files/documents/closing_letters/google-inc./admob-inc/100521google-admobstmt.pdf, European Commission decision of 6 December 2016 in Case M.8124 - Microsoft / LinkedIn, http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf, European Commission decision of 21 December 2016 in Case COMP/M.8180 - Verizon / Yahoo, http://ec.europa.eu/competition/mergers/cases/decisions/m8180_240_3.pdf, Anticipated acquisition by Facebook Inc of Instagram Inc, UK Office of Fair Trading File Number ME/5525/12 (22 August 2012), https://assets.publishing.service.gov.uk/media/555de2e5ed915d7ae200003b/facebook.pdf, Closing Letters Federal Trade Commission in Facebook, Inc. / Instagram, Inc. FTC File No. 121-0121 (August 22, 2012), https://www.ftc.gov/enforcement/cases-proceedings/closing-letters/facebook-inc-instagram-inc.

[80] European Commission decision of 11 March 2008 in Case COMP M.4731 – Google / DoubleClick, http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf, Statement of the Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170 (December 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf, European Commission decision of 6 December 2016 in Case M.8124 - Microsoft / LinkedIn, http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf, European Commission decision of 21 December 2016 in Case COMP/M.8180 - Verizon / Yahoo, http://ec.europa.eu/competition/mergers/cases/decisions/m8180_240_3.pdf.

it,[81] but the acquisition never went through.[82] Had it happened, it would no doubt have been included on our shortlist. Thus, we decided to include the European Commission's review of this transaction in our analysis.

As can be seen in the table below (**Table C**), we then focused our analysis on the four clearance decisions identified as per above and on the European Commission's decision in *Microsoft/Yahoo*.

Table C: New 1st party combinations, Prevalence, US FTC and EU Commission merger reviews per transaction

Legend	Filings documented	Filings pertinent to this analysis

	Year	Target	Acquirer	FTC	EU Commission
1.	2006	**Youtube**	**Google**	Routine Filing	No Filing
2.	2014	**Firebase**	**Google**	No Filing	No Filing
3.	2009	**Admob**	**Google**	**Merits Review**	No Filing
4.	2012	**Instagram**	**Facebook**	**Merits Review**	No Filing **(UK Merits Review)**
5.	2007	**DoubleClick**	**Google**	**Merits Review**	**Merits Review**
6.	2014	**Liverail**	**Facebook**	Routine Filing	No Filing
7.	2013	**Mopub**	**Twitter**	Routine Filing	No Filing
8.	2013	**Crashlytics**	**Twitter**	No Filing	No Filing
9.	2017	**Yahoo**	**Verizon**	No Filing	**Merits Review**
10.	2016	**Linkedin**	**Microsoft**	No Filing	**Merits Review**
11.	2014	**Bitstadium**	**Microsoft**	No Filing	No Filing
12.	2014	**Flurry**	**Verizon**	Routine Filing	No Filing
13.	2015	**Appnexus**	**Yieldex**	No Filing	No Filing
14.	2014	**Bluekai**	**Oracle**	Routine Filing	No Filing

[81] European Commission decision of 21 December 2016 in Case COMP/M.5727 - MICROSOFT/ YAHOO! SEARCH BUSINESS, http://ec.europa.eu/competition/mergers/cases/decisions/M5727_20100218_20310_261202_EN.pdf. The US FTC cleared the merger on 17 February 2010 (Acquisition of Microsoft Corporation by Yahoo! Inc., FTC File No. 20090650 (February 17, 2010), https://www.ftc.gov/enforcement/premerger-notification-program/early-termination-notices/20090650).

[82] *See* some of the history here: https://searchengineland.com/library/features/microsoft-yahoo-merger.

15.	2017	**Moat**	**Oracle**	Routine Filing	No Filing
16.	2015	**Maxymiser**	**Oracle**	No Filing	No Filing
17.	2016	**Addthis**	**Oracle**	Routine Filing	No Filing
18.	2015	**Datapop**	**Criteo**	No Filing	No Filing
19.	2014	**Adquantic**	**Criteo**	No Filing	No Filing
20.	2014	**Tedemis**	**Criteo**	No Filing	No Filing
21.	2014	**Adcolony**	**Opera**	No Filing	No Filing
22.	2013	**Umeng**	**Alibaba**	No Filing	No Filing
23.	2014	**Rocketfuel**	**Xplus Two**	No Filing	No Filing
24.	2016	**Flashtalking**	**Encore Media Metrics**	No Filing	No Filing
25.	2017	**Intowow**	**Verizon**	No Filing	No Filing
26.	2011	**Sizmek**	**Vector Capital**	No Filing	No Filing
27.	2016	**Tube Mogul**	**Adobe Systems**	Routine Filing	No Filing
28.	2016	**Livefyre**	**Adobe Systems**	No Filing	No Filing
29.	2011	**Typekit**	**Adobe Systems**	No Filing	No Filing
30.	2018	**aerserv**	**inmobi**	No Filing	No Filing
31.	2017	**Flickr**	**Verizon**	No Filing	No Filing
32.	2017	**Tumblr**	**Verizon**	Routine Filing	No Filing
33.	2017	**Millenialmedia**	**Verizon**	Routine Filing	No Filing
34.	2016	**krux**	**salesforce**	Routine Filing	No Filing
35.	2017	**Brightroll**	**Verizon**	Routine Filing	No Filing
36.	2017	**One By Aol**	**Verizon**	Routine Filing	No Filing
37.	2017	**Gravity Insights**	**Verizon**	No Filing	No Filing
38.	2010	**Admarvel**	**Opera**	No Filing	No Filing
39.	2017	**Aol**	**Verizon**	Routine Filing	No Filing
40.	2011	**Demdex**	**Adobe Systems**	No Filing	No Filing
41.	2017	**Radium One**	**RhythmOne**	No Filing	No Filing
42.	2016	**Tapad**	**Telenor**	Routine Filing	No Filing

Through this analysis, we found that although the transactions most scrutinized by competition authorities broadly correlate with prevalence measures, many transactions that appear relevant using prevalence measures were not the subject of competition scrutiny. This is likely largely due to the revenue share thresholds being not significant enough to trigger scrutiny. Further, competition authorities have considered third party tracking related harms only in rare instances, i.e. when they could be subsumed within mainstream antitrust analysis. Authorities have considered a limited range of cases, such as the ones discussed below, where the data aspects could be framed as questions about the effects of merging two previously separate databases to strengthen the merged entity's market power, or as questions of competitive constraints represented by each of the merging parties' datasets on the other party.[83] Even in the cases below, authorities dismissed data concentration, and any associated privacy concerns, on grounds that (a) the merger would generate a number of competitive efficiencies in terms of innovation and product quality,[84] (b) the market for user data is very competitive and/or the merging parties are small players on the advertising market,[85] (c) the data being collected is not "unique",[86] (d) the data provided to advertisers contractually is limited, e.g. it only relates to use of the webpage where advertising is served,[87] and/or contractual agreements limit the availability of party data to third parties, so there is no real "market effect".[88]

To add to the discussion in Part III above, there has been substantial reflection recently on the overlaps and tensions between competition law on the one hand, and privacy, data protection, consumer protection on the other.[89] Competition

[83] For another instance of this method, albeit not in relation to third party tracking, see European Commission decision of 6 September 2010 in Case COMP/M. M.8788 - APPLE / SHAZAM, in which the Commission cleared the merger after an advanced investigation. For a commentary see Nicolò Zingales, *Apple/Shazam: Data Is Power, But Not A Problem Here* CPI EU NEWS (Dec. 2018), https://www.competitionpolicyinternational.com/appleshazam-data-is-power-but-not-a-problem-here/#_edn27.

[84] European Commission decision of 21 December 2016 in Case COMP/M.5727 - MICROSOFT/ YAHOO! SEARCH BUSINESS, http://ec.europa.eu/competition/mergers/cases/decisions/M5727_20100218_20310_261202_EN.pdf.

[85] European Commission in Microsoft / LinkedIn, *supra* note 37.

[86] European Commission decision of 21 December 2016 in Case COMP/M.8180 - Verizon / Yahoo, http://ec.europa.eu/competition/mergers/cases/decisions/m8180_240_3.pdf.

[87] European Commission in Google /DoubleClick, *supra* note 14.

[88] European Commission in Microsoft/LinkedIn, *supra* note 37.

[89] *See e.g.* European Data Protection Supervisor, *Privacy and Competitiveness in the Age of Big Data* (March 2014), https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en; European Data Protection Supervisor, *Big Data and Digital Clearinghouse*, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en; OECD, *Big Data: Bringing Competition Policy to the Digital Era*, DAF/COMP(2016), 27 October 2016, https://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm; Autorité de la concurrence and Bundeskartellamt, *Competition Law and Data*, 10 May 2016, http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf; MAURICE E STUCKE & ALLEN P GRUNES, BIG DATA AND COMPETITION POLICY (2016); ARIEL EZRACHI AND MAURICE E STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016); Allen P Grunes, *Another Look at Privacy*, 20 GEORGE MASON L REV 1107 (2013); Ariel Ezrachi, *The Goals of EU Competition Law and the Digital Econom*, BEUC DISCUSSION PAPER (2018).

authorities and scholars have tended to resist the idea that privacy should be a matter of concern for competition authorities,[90] yet on the other hand, a new literature is developing which argues that competition authorities should take on policy goals beyond consumer welfare, including inequality, labor,[91] and also importantly privacy and data power.[92]

In what follows we analyse the language and reasoning of competition authorities in the five cases we identified. The cases are presented in chronological order. They were decided against a backdrop of shifting and conflicting understandings about the relationship between antitrust and privacy aspects of mergers in the digital sector. They show that competition authorities until recently have largely failed to incorporate the importance of data and privacy into the competition analysis, and, crucially, have glossed over third party tracking-related questions, focusing instead on first party data. The importance of privacy aspects is particularly salient in mergers and acquisitions between companies engaged in third party tracking because these mergers can have effects on companies' ability to track and profile individuals as well as increase the merging entities' market share. These considerations are however hardly captured in mainstream antitrust analysis because data is gathered in the absence of a clear contractual relationship with the end-user.[93]

The recently issued German Bundeskartellamt decision against *Facebook*[94] however suggests that something may be gradually changing in competition authorities' approach toward data in third party tracking markets. In what follows we trace, case-by-case, a very slow – and far from complete - evolution towards a greater awareness of data and privacy issues.

---

[90] Darren S. Tucker & Alexander Okuliar, *Internet Ready: Agency Enforcement of Online Mergers*, 26 ANTITRUST 80 (2011) ("Despite repeated calls from some public interest groups, the agencies have not incorporated consumer protection considerations like privacy into their analysis of Internet (or other) mergers" at 83); Maureen K Ohlhausen and Alexander P Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L J 121 (2015).

[91] *See e.g.* FTC Chairman Joe Simons' introductory remarks on September 13th, 2018, *Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century*, https://www.ftc.gov/policy/hearings-competition-consumer-protection, and Maurice Stucke, *Reconsidering Antitrust's Goals*, 53 BOSTON COLLEGE LAW REVIEW 551, 611 (2012), https://lawdigitalcommons.bc.edu/bclr/vol53/iss2/4.

[92] Francisco Costa-Cabral and Orla Lynskey, *Family Ties: The Intersection between Data Protection and Competition in EU Law* 54 CML REV 11 (2017); Maurice Stucke, *Should We Be Concerned About Data-opolies?* 2 GEO. L. TECH. REV. 275 (2018), Orla Lynskey, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 THEORETICAL INQUIRIES IN LAW 189 (2019).

[93] On this see below and also Ariel Ezrachi & Viktoria H.S.E. Robertson, *Competition, Market Power and Third-Party Tracking*, 42 WORLD COMPETITION 5 (2019)

[94] *See* Bundeskartellamt [BKA] [Federal Cartels Office] *Prohibition Decision: Facebook Inc. i.a. - The use of abusive business terms pursuant to Section 19 (1) GWB* (2 June 2019) (Germ.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568.

5.1 Google/DoubleClick

As mentioned above, the *Google/DoubleClick* merger generated two full merits reviews, one by the European Commission and one by the US FTC.[95] Both authorities analyzed the merger's horizontal and vertical competition risks, reaching broadly similar conclusions. Four points are worth noting on these two investigations.

The first is that both authorities expressly stated that their decision is without prejudice to any data protection and privacy legislation, and also that the relevant data privacy aspects had to be dealt with separately and are not for competition authorities to address. In particular it is worth noting that during the EU investigation, a large number of market participants and civil society groups voiced concerns that the proposed concentration would violate privacy rules.[96] Such concerns focused on the effects of combining the parties' datasets. The European Commission's approach in that case was to treat privacy as distinct from competition law aspects.[97]

The second point to note is that the European Commission in its decision described third party tracking activities in detail, without however calling them a "market" or using the expression "third party tracking", explaining the activities of entities that collect data from third party websites as part of delivering ad serving tools.[98] Compared to the other European Commission decisions we looked at, here the Commission was thorough on the data collection aspects and on data's effect on the merging parties' market position.

The related third point is that both the European Commission and the Federal Trade Commission examined a theory of harm according to which the combination of Google and DoubleClick's databases would give the integrated entity an overwhelming advantage over other competitors. The competitors were understood as being other ad intermediaries by the FTC,[99] and possibly also entities offering bundled intermediation and ad serving tools by the European Commission.[100] While the European Commission described the data collection aspects in greater detail, both authorities agreed that the merger would not increase the merged entity's power on the relevant market(s), mainly on contractual grounds. In the following passage, the European Commission explained some of the harms at stake, stating that contractual restrictions were in place which could prevent the databases from being merged:

---

[95] Federal Trade Commission in Google / DoubleClick, *supra* note 17, European Commission in Google/ DoubleClick, *supra* note 14.
[96] Julia BROCKHOFF et al., *Google/DoubleClick: The first test for the Commission's non-horizontal merger guidelines*, COMPETITION POLICY NEWSLETTER 53, 59 (2008), http://ec.europa.eu/competition/publications/cpn/2008_2_53.pdf.
[97] *Id. supra*.
[98] European Commission in Google/DoubleClick, *supra* note 14, at paras. 181-189, 255-267.
[99] Federal Trade Commission in Google / DoubleClick, *supra* note 17, at 12 and following.
[100] *See* European Commission in Google / DoubleClick, *supra* note 14, at paras 359 and following.

> It is not excluded that, from a factual point of view, the merged entity would be able to combine DoubleClick's and Google's data collections. Such a combination, using information about users' IP addresses, cookie IDs and connection times to correctly match records from both databases, could result in individual users' search histories being linked to the same users' past surfing behaviour on the internet.... The notifying party submitted that DoubleClick's current contracts with advertisers do not allow the use of data regarding which web pages a user visited, in order to better target ads from other advertisers than those that were instrumental in bringing this data into existence … the merged entity would also be contractually prevented from using that part of its enlarged database originating from DoubleClick to improve, for example, targeting of search ads on Google's sites …. However, these contracts could be waived, modified or renegotiated.[101]

Reliance on contractual agreements seems a weak basis for dismissing competition concerns about increases in market power,[102] or loss of competitive constraints on a given data-sensitive market.

The final point to note in relation to this case is that in the FTC procedure, two Commissioners issued separate statements, both emphasizing the privacy implications of the merger, and adding interesting comments on the future of merger control in the digital sector. Commissioner Leibowitz commented that privacy issues "clearly transcend" the antitrust issues in this case.[103] In his view "*the Commission should consider how to address these privacy issues across industries and from multiple perspectives.*"[104] Stating that "*if the online industry does not adequately address consumer privacy through self-regulatory approaches, it may well risk a far greater response from government,*"[105] Commissioner Harbour dissented in the FTC decision because of her belief that the merger could have a far-reaching negative impact on consumers.[106] She argued that the FTC should have imposed some remedies on the merging parties, using the full scope of its statutory powers under section 5 of the FTC Act, a section that empowers it to act both to protect competition and consumer welfare. Her view was that the FTC relied instead on a traditional understanding of competition, which led it to dismiss the case without privacy safeguards for consumers. On the question of privacy, she noted that:

> senior corporate officials have offered assurances that the combined firm will not use consumer data inappropriately… I am uncomfortable accepting the merging parties' nonbinding representations at face value… the merger

[101] *Id. supra.* at para. 360-362.
[102] In the EU Horizontal Merger Guidelines, *supra* note 51, at 5, "*market power*" is defined as "*the ability of one or more firms to profitably increase prices, reduce output, choice or quality of goods and services, diminish innovation, or otherwise influence parameters of competition*," https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52004XC0205%2802%29.
[103] Concurring Statement of Commissioner Leibowitz in the Google/DoubleClick Matter, FTC File No. 071-0170 (December 20, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/concurring-statement-commissioner-jon-leibowitz-google/doubleclick-matter/071220leib_0.pdf.
[104] *Id. supra*.
[105] *Id. supra*.
[106] Dissenting Statement of Commissioner Harbour In the Matter of Google/DoubleClick, FTC File No. 071-0170 (December 20, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf.

> creates a firm with vast knowledge of consumer preferences, subject to very little accountability.[107]

She added:

> Traditional competition analysis of Google's acquisition of DoubleClick fails to capture the interests of all the relevant parties. Google and DoubleClick's customers are web-based publishers and advertisers who will profit from better-targeted advertising. From the perspective of these customers, the more data the combined firm is able to gather and mine, the better... But this analysis does not reflect the values of the consumers whose data will be gathered and analyzed. Under the majority's application of Section 7[108], there is no adequate proxy for the consumers whose privacy is at stake, because consumers have no business relationship with Google or DoubleClick.[109]

Commissioner Harbour's dissenting statement reflects some of the concerns which this paper highlights with the human and social impacts of data mergers in the third party tracking industry. The FTC and the European Commission generally take different approaches to competition law enforcement, particularly in non-merger cases. The influence of Chicago School economics on US antitrust authorities' approach has contributed to their tolerance toward large monopolies and conglomerates of power, including those that license enormous concentrations of data power. In the EU, instead, protection against monopoly power is a routine concern. Abuses of monopoly or oligopoly power are prohibited under Article 102 of the Treaty on the Functioning of the EU.[110] This ideological difference often results in the European Commission taking a bolder stance toward conglomerates of economic power in both mergers and unilateral behavior cases. In this particular instance, however, it seems that the approach of the two authorities was similar and that the FTC procedure allowed its Commissioners to display greater sensitivity toward privacy concerns, albeit mostly in the form of a dissent.

However, despite this notable discussion of third party data (and the privacy risks raised by Commissioner Harbour), in subsequent cases authorities have generally glossed over third party data. One reason for this may be that DoubleClick's business model was from its inception centered on third party tracking, making the issue unavoidable. Instead, the subsequent cases, discussed below, concerned firms that had both first and third party data. In these, authorities chose to focus their arguments almost exclusively on the former, to the exclusion of the latter.

---

[107] *Id. supra*, at 9-10.

[108] United States Clayton Act, 15 U.S.C. § 18 (2012), prohibits mergers and acquisitions where the effect "*may be substantially to lessen competition, or to tend to create a monopoly.*"

[109] Dissenting Statement of Commissioner Harbour, *supra* note 115, at 10.

[110] For a broader discussion of the US approach towards monopolies in the digital sector, see eg. Maurice Stucke, *Should We Be Concerned About Data-opolies?* 2 GEO. L. TECH. REV. 275 (2018), https://www.georgetownlawtechreview.org/should-we-be-concerned-about-data-opolies/GLTR-07-2018/.

5.2 Microsoft/Yahoo

This case concerns Microsoft's proposed acquisition of Yahoo's internet search and search advertising businesses. Had it gone through, the acquisition would have led to the merger of the second and third largest search engines in the EEA at that time. Although it would have constituted a (welcome) competitive constraint on Google's market power on web search, the merger also had the potential to generate significant privacy harms for individuals subject to third party tracking. Yet the language of privacy or data protection does not appear in the decision. This decision represents a symptomatic example of an early EU Commission's failure to understand or acknowledge the privacy harms at stake.[111]

In the decision, the European Commission does mention the third party tracking-related aspects of online advertising a number of times. For instance, the Commission refers to APIs as "*syndication agreements*" which enable "*third party publishers to use a search engine's technology and an ad platform's pool of ads to deploy internet search services and search ads … onto their websites.*"[112] The Commission also describes behavioral targeting across the web:

> A growing number of both search and non-search ads are also behaviourally targeted. … Information on that user behaviour is collected by using so-called "cookies".[113]

However the term "*user behavior*" ignores the question of whether the targeting also includes tracking of individuals who are not users of the relevant first party service (i.e. Microsoft or Yahoo) on the wider web. This is despite the fact that both firms were active in the third party tracking market at the time.[114]

Most interesting however is the Commission's treatment of the possible anticompetitive harms at stake. The transaction would have entailed the merger of the second and third largest search engines in the EEA, and thus could have led to the creation of a very large combined database of individual searches. The Commission decision does not however mention the potential risks from a privacy perspective, nor the question of whether the quality of search could be affected negatively by an increase in the data available to the merging parties and advertisers. Instead, the Commission analysed only the potential price and quality benefits the merger could bring about.[115]

Examining in turn the effects of the merger on advertisers, publishers and distributors of advertising, the Commission indeed pointed out that all interested parties welcomed the transaction as a positive constraint on Google's search dominance.[116] This is not surprising as all these stakeholders have an interest in

---

[111] European Commission in MICROSOFT/ YAHOO! SEARCH BUSINESS, *supra* note 49.
[112] *Id.*, at paras 51-52.
[113] *Id. supra*, at para 40.
[114] *See* Stephanie Clifford, "*Instant Ads Set the Pace on the Web",* NEW YORK TIMES, *March 11, 2010.* https://perma.cc/NRB5-ZQLA

[115] *Id.*, eg. at para 192.
[116] *Id.*, at paras 196-198.

accessing more personal data on competitive terms. Here less concentration on the search market meant cheaper access to search data for those who use it to target ads.

As to the merger's effects on internet search users, on the other hand, one would have expected a recognition of potential data-related harms. Instead, the Commission focused once again on the positive effects of scale on algorithmic search *"relevance"*[117] and content variety,[118] instead of privacy. To a mainstream competition lawyer the decision looks perfectly anodyne. However if one looks at the decision through the lens of our current understanding of surveillance capitalism and algorithm-driven competition,[119] privacy seems an important omission.

In this decision, privacy harms represented by greater access to data by third party trackers are not only viewed as irrelevant to the competition analysis, but are overtly ignored. This is symptomatic of a more general predisposition of competition authorities' to neglect the non-monetary value of data in the third party tracking industry, focusing instead on short term productive efficiencies and neglecting long term distributional implications. By overtly omitting privacy considerations, the Commission in fact has failed to fulfill its mandate to protect consumer welfare (which, as argued above, must be understood as encompassing more than just price and quality of search), while also protecting and celebrating potentially harmful data reliant business models in the advertising ecosystem.

5.3 Microsoft/LinkedIn

In its *Microsoft/LinkedIn* decision,[120] the European Commission is more concerned about potential data harms to consumers and competition while not going as far as considering third party tracking issues. It identified two possible theories of harm resulting from the combination of Microsoft and LinkedIn's respective databases. Harm could arise if the datasets increased the merged entity's market power on the market for such data, impeding access to new entrants; or if the two entities were previous competitors on the basis of their data, and stopped competing as a result of the merger.[121] However according to the Commission the possibility of such harms did not arise in this case for three reasons: first, neither Microsoft nor LinkedIn made available their data to third parties for advertising purposes, with very limited exceptions. Second, the market for valuable internet user data available for advertising purposes was so competitive that the combined dataset would not be capable of excluding third parties from the online advertising market. Third, Microsoft and LinkedIn were both small players on the online advertising market and competed with each other only to a very limited extent.[122]

---

[117] *Id.*, at para 223.
[118] *Id.*, at para 202.
[119] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019); ARIEL EZRACHI AND MAURICE STUCKE, VIRTUAL COMPETITION, THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016).
[120] European Commission in Microsoft / LinkedIn, *supra* note 37.
[121] *Id. supra*, at para 179.
[122] *Id.*, at para 180.

The Commission's reasoning here appears too narrow in three respects. First, the assumption that if the parties do not sell data to others there is no "market effect" is flawed: internal use of data by an entity can have a huge impact on consumers, e.g. use of data in the creation of profiling or the training of AI models has value even when the data isn't sold. Facebook for instance offers advertisers the highly valued possibility to target ads to specific groups of users that Facebook has pre-identified but does not offer these advertisers access to any raw or individualized data about the users. Following the Commission's reasoning, it could be argued that Facebook's use of data for advertising purposes does not have a direct market effect on advertisers. This reasoning would be unsustainable. Second, stating that the online advertising market is competitive because players can access a lot of valuable data that is not controlled by Microsoft or LinkedIn does not justify the claim that merging the two databases would have no significant impact on consumers: merging data can have implications for consumers because of the increased profiling and behavioral targeting capabilities of the merged entity, even if there is no harm to other competitors. Finally, the Commission in its decision appears to emphasize the fact that parties are contractually prevented from sharing data with third parties, without sufficiently investigating the potential of any future breaches of or amendments to those contracts, or imposing remedies in that regard.

5.4 Verizon/Yahoo

The same two theories of harm were discussed by the Commission in its *Verizon/Yahoo* merger decision, another of the decisions we identified through our methodology:[123] barriers to entry for competitors as a result of increased market power on the data market; or the two entities were previous competitors on the basis of their data, and stopped competing as a result of the merger. In addition to the grounds provided in Microsoft/LinkedIn for why such harms do not arise in this case, the Commission added:

> the vast majority of respondents to the market investigation indicated that the data collected by Yahoo and Verizon cannot be characterised as unique. Similar to other providers of online advertising services, Verizon and Yahoo are able to capture and utilise data to better target online advertising. One customer noted that it expects the merged entity to be able to improve its data capability which in turn would improve its competitiveness against existing stronger competitors.[124]

In other words, the merger would not allow the parties to create unusual or unique profiles, but only profiles that could equally be generated on the basis of existing available data. Even if this were factually true, which would be very difficult to prove, this would not extinguish any anti-competitive or data protection concerns about the merger: the more proprietary data an entity controls, the more it can use it to its advantage on the market. This point was left unaddressed by the European Commission in its decision.

[123] European Commission in Verizon / Yahoo, *supra* note 87.
[124] *Id. supra*, at para 93.

5.5 A gradual shift to pluralism, but third party data still amiss

To summarize the conclusions of this section: while we note a progression of competition authority's approach from complete neglect of the non-market value of data to a progressive incorporation of data concerns into the merger review analysis, regulators have overlooked several key aspects involved in consolidation between third party trackers. First, only a small number of the most significant consolidations (in terms of data consolidation) were reviewed at all, and an even smaller number were reviewed in depth. This prompts us to consider whether alternative measures or thresholds are needed to ensure that important data-sensitive mergers are reviewed by regulators.

Second, aside from a small number of cases which we shortlisted as delving more deeply into the data issues (*Google / DoubleClick*, *Yahoo/ Verizon*, and *Microsoft/LinkedIn*), aspects of third-party tracking that are problematic from a competition standpoint and that have been identified in previous sections seem to have been disregarded or simply missed. Further, even in those cases where third party aspects were addressed, no investigation of the prevalence, prominence and nature of the first party websites or apps on which each third party tracker was present, appears to have been proposed or made. Not to mention the fact that in none of these cases we found tracking or data collection activities described as a relevant market or specific sector of economic activity, save for *Google/DoubleClick* where authorities described these activities as merely ancillary to advertising markets.

The third omission is intentional rather than accidental; regulators have more often than not explicitly ruled out consideration of privacy and data protection aspects of these mergers as outside the scope of competition law. The *Facebook/WhatsApp* merger decision,[125] while it does not tackle issues of third party tracking, illustrates antitrust authorities' reluctance to engage with data protection considerations.[126] In *Google/DoubleClick*, Commissioner Harbour's dissenting opinion is the exception that confounds the general trend.

Overall, this analysis appears to confirm that competition authorities' approach to mergers in the data sector is limited by an excessive focus on economic concerns to the detriment of a holistic analysis of the harms and benefits that may result from these mergers for consumers and society. A pluralist approach which takes the impacts of data collection and use seriously in an analysis of economic and societal effects would be welcome going forward. Indeed antitrust authorities should be readier to embrace complexity and bolder in analyzing the effects of mergers that have an impact on privacy, instead of hiding these concerns behind an appearance of disciplinary coherence and neutral language. The German Bundeskartellamt's approach in its *Facebook* investigation appears to be moving in this direction.

**

[125] European Commission in Facebook / Whatsapp, *supra* note 24.

[126] *Id. supra*, at para 164: "*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*."

VII. CONCLUSIONS

Commissioner Harbour's dissenting position over *Google / DoubleClick* has proved prescient. In the years since the acquisition, the Alphabet companies (including Google and DoubleClick) have expanded the reach of their third party tracking capability to encompass the majority of all websites and apps on the Android platform.[127] As this paper attests, recent years have seen numerous significant consolidations amongst other firms which engage in third party tracking. The third party tracking aspects of these mergers and acquisitions raise additional complications which have not been reflected in the existing discussion about the relationship between data accumulation, competition, and data protection. The way these issues will be addressed in future depends on evolving institutional views about the relationship between competition and data protection. The analysis above points to several shortcomings of existing approaches, and suggests the need for certain new elements as part of regulators' approaches in future.

Traditional thresholds for review may need supplementing with new measures: the current approach is one in which reviews are triggered by market share and turnover thresholds, not thresholds accounting for power and control over data. This leads authorities to fail to review certain mergers which might be highly significant in terms of the data combined, even if one or both firms do not have a significant market share or significant revenue measured in monetary terms. Under the current turnover and market share-based tests, large data-mergers are often missed. In Germany and Austria, new thresholds have been introduced based on the value of a transaction instead of turnover.[128] The intention behind the new legislation appears to be to move beyond the current focus on monetized flows toward a more comprehensive consideration of yet-to-be-monetized data flows.[129] Even taking into account this and similar recent evolutions in merger control procedure, at present competition authorities' merger reviews still take little or no account of the extent and nature of third party data tracking in merger transactions, they don't investigate significance or prevalence of third party trackers' activities on web or mobile. This in our view should change.

Data protection and competition might sometimes pull in opposite directions regarding third party tracking. In spite of embracing a pluralist view of antitrust regulation and considering that better competition law enforcement and greater

---

ach of these entities on the Apple iOS platform is unknown, due to the Apple distribution and security model making large scale empirical research impractical.

[128] German Competition Act [GWB] § 35 para. 1(a) and Austrian Cartel Act 2005 [KartG] § 9(4), and also see the Austrian and German competition authorities' joint *Guidance on Transaction Value Thresholds for Mandatory Pre-merger Notification*, July 2018, at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Leitfaden/Leitfaden_Transaktionsschwelle.pdf;jsessionid=52642E8F030992776E405857B344C7E9.1_cid362?__blob=publicationFile&v=2.

[129] Bundeskartellamt [BKA] [Federal Cartels Office] *Press Release on Joint guidance on new transaction value threshold in German and Austrian merger control submitted for public consultation* (14 May 2018) (Germ.), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2018/14_05_2018_TAW.pdf?__blob=publicationFile&v=2.

privacy protection generally go hand in hand, we recognize that privacy and competition law may sometimes conflict when certain options are compared.

Consolidation between third party trackers could be both positive and negative for privacy. On the one hand, the more websites or applications a particular third-party tracker is integrated with, the more comprehensive and revealing the profiles it can build, the more data concentration. On the other hand, an increase in the number of third parties can lead to more tracking of individuals, whilst also reducing market concentration. There may therefore be a trade-off in some cases between reducing the overall number of tracking firms to which an average individual is exposed, and reducing the amount of different data types that any one tracker can amass about a given consumer.

Because of the nature of third party tracking technology and business models, forms of market activity that are acceptable or even positive from a competition law perspective may thus at times fall short of desirability from a data protection perspective. When this occurs, it is important for competition and data protection authorities to engage in a collaborative dialogue. The starting point for such dialogue, we maintain, must be the values to be protected and the harms to be avoided, not disputes around disciplinary boundaries and exclusive competencies.

The nature of data combination is more complicated to ascertain in the case of third party mergers: Consolidations between firms who collect their data directly from users - such as Facebook (in its capacity as a social network provider) and WhatsApp - are easier to scrutinize because the first party data is limited and known. But firms who operate third party tracking networks collect their data indirectly via first parties, and it may therefore be difficult to know exactly the volume and variety of data being combined as a result of mergers between them. This perhaps explains why in the decisions that we analyzed competition authorities focus on the first-party rather than third-party data collection by those firms.

But a merger between third party trackers does not just affect users of two services, it affects all users of all the multiple different services on which each tracker is present pre-merger. In many cases, third party trackers may not even be able to fully audit which sites or apps they are present on. Thus, even if authorities have on some occasions considered the effects of merging different data sources, they have generally failed to do this thoroughly, even in significant cases like *Verizon / Yahoo*. A full audit of all first party data sources, and the effects of combining them, is indeed a significant undertaking, because of the sheer number and variety of combinations, but a necessary one when assessing the effects of combining the two datasets.

Timing and regulation: mergers in the digital sector are characterized by dynamic markets, transient products, changing data and evolving needs. The challenge for regulators across the competition and data protection spectrum is to minimize unnecessary and time-consuming burdens while ensuring effective regulation. While this balance is very difficult to strike, if an investigation is complex and time-consuming it is important that regulators consider timeliness and long-term

effects. A long investigation that focuses on short term costs and benefits has a high likelihood of leading to costly, misguided results.

Maintaining a static division between purist visions of competition law and data protection risks rendering both irrelevant. A discipline or regulatory authority becomes obsolete if it stops addressing needs of societal importance. Accordingly, antitrust and data protection regulators' concern to stick to the foundations of their disciplines may at times prevent them from tackling important issues in evolving digital markets. As we have seen, competition regulators often fail to address important issues in third party tracking because of their focus on economic notions of "market effect" "market share" "turnover" "consumer welfare" "efficiency" and so on, as well as a concern that their discipline is being co-opted to achieve non-competition aims.[130]

Similarly, data protection regulators often overlook important M&A issues as a result of their lack of familiarity with merger issues. For example, the fact that two companies have complied with their data protection obligations does not mean that an entity resulting from their merger will also automatically be compliant with data protection.

Joining forces. As competition, data and consumer protection regulators struggle to refine and distinguish their respective competences, a few recent evolutions appear to be offering a way forward. First, the Bundeskartellamt's is showing that a bolder stance of antitrust regulators toward issues that involve data protection is granted:

> Where access to the personal data of users is essential for the market position of a company, the question of how that company handles the personal data of its users is no longer only relevant for data protection authorities. It becomes a relevant question for the competition authorities, too. … Monitoring the data processing activities of dominant companies is … an essential task of the competition authority which cannot be fulfilled by a data protection authority.[131]

Second, discussions are starting on the need for one-stop-shop regulators whose role would be to monitor digital companies' behavior toward individuals by combining antitrust, data protection, contract and consumer protection perspectives.[132] As a landscape of new possibilities emerges from the fog of consumer-welfare centered merger analysis, we still need the political will to adopt a bolder stance on these questions.

---

[130] Orla Lynskey, *At the crossroads of data protection and competition law: time to take stock* 8 INTERNATIONAL DATA PRIVACY LAW 179 (2018).

[131] Bundeskartellamt [BKA] [Federal Cartels Office] *Background information of the Facebook proceeding* (19 December 2017), (Germ.), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6.

[132] *See* eg. Inge Graef et al., *Fairness and enforcement: bridging competition, data protection, and consumer law*, 8 INTERNATIONAL DATA PRIVACY LAW 200 (2018), where the authors argue that relying on the notion of "fairness," a notion that underlies competition, data protection, and consumer law, could lead to an alignment of substantive protections and enforcement mechanisms in these three fields.

Acknowledgements
We would like to thank the editor and two anonymous reviewers for insightful feedback on the first draft of this paper. Reuben Binns would like to acknowledge funding from the PETRAS IoT Hub Strategic Fund, funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant number N02334X/1.