

Competition, Market Power and Third-Party Tracking

Ariel Ezrachi* and Viktoria H.S.E. Robertson†

The prevalence of third-party tracking in our modern ecosystem cannot be ignored. Trackers, on our websites and apps, enable multi-sourced data gathering, at distinct volume, velocity, verity and veracity. While operated by numerous operators, the majority of these trackers are controlled by a handful of data giants. In this paper we consider the rise and growth of this industry, the power it has bestowed on a handful of operators, and the possible implications for consumer welfare and competition.

I. Introduction

The online digital landscape has benefitted us with waves of innovation, transforming the way we search, shop, communicate and consume information. Be it on our computer, tablet or mobile device, the world is our oyster. A key characteristic of our online world is the ability to offer us what we most desire. Targeted ads, targeted news, targeted goods and services.

‘Targeted everything’ is the new norm which supports our online (and offline) ecosystems. The ability to harvest data, analyse and react has become a significant pillar that delivers efficiencies and value for platforms, sellers, advertisers, content providers and consumers. The power to gather information on the use of apps and services, identify shopping and behavioural patterns, and monitor consumption of media and news enables our ecosystem to deliver levels of transparency which are unmatched by the old brick and mortar world. It enables intelligent investment, development of new services and products, segmentation, personalisation and better optimisation of our online world. More of what we want, when we most want it.

These distinct benefits have come at a cost. The quest to better map our behaviour, our social relations and desires can adversely affect our autonomy and privacy. Furthermore, the use of tracking, in particular in stealth mode, has led to asymmetry in the relationship between users and providers and has enabled possible price and behavioural discrimination – the ability to exploit and extract value from unsuspecting consumers by estimating their willingness to pay in real time.¹ Also noteworthy are possible effects these new tools have had on the manipulation

* Slaughter and May Professor of Competition Law, The University of Oxford. Director, The University of Oxford Centre for Competition Law and Policy. Email: ariel.ezrachi@law.ox.ac.uk.

† Assistant Professor, Institute of Corporate and International Commercial Law, University of Graz. At the time of writing also academic visitor at the University of Oxford Centre for Competition Law and Policy and the Institute of European and Comparative Law. Email: viktoria.robertson@uni-graz.at.

¹ Frederik Zuiderveen Borgesius and Joost Poort, ‘Online Price Discrimination and EU Data Privacy Law’ (2017) 40 J of Consumer Policy 347; Jerry Usem, ‘How Online Shopping Makes Suckers of Us All’ *The Atlantic* (May 2017); Arwa Mahdawi, ‘Spotify Can Tell If You’re Sad. Here’s Why That Should Scare You’ *The Guardian* (16 September 2018).

of news feeds, search results, the rise of echo chambers, and, more broadly, the market for ideas.²

The increased significance of data (that feeds the big analytics machines) has also affected the relationship between market operators. It influences market dynamics, the nature of entry and expansion barriers, and the power of those in possession of quality data. It also gave rise to new functions linked to data collection and processing. One of them, which is at the centre of this paper, is that of third-party trackers.

In what follows, we consider the rise and growth of this industry and the power it has bestowed on a handful of operators. Our analysis sets out to illustrate the significant role these operators have in the market for data and explore possible implications to competition dynamic and consumer welfare.

II. The Prevalence of Third-Party Tracking

Third-party tracking is a mechanism through which a company (the third-party tracker) hooks onto another (first-party) website or application and collects identifiable data about users, which enables it to build a comprehensive profile about them.³ Third-party tracking often occurs when a (first-party) website embeds content from a third party, thereby enabling this third party to track the online behaviour of the first party's users.⁴ Tracking may be done both actively and passively.⁵ It may offer generic information on usage and webpage visits, or combined and analysed information which enables the identification of the individual.⁶ In many cases, a user's identity transpires from the first party to the third party.⁷

The gathering of personalised data – through third-party tracking or otherwise – is primarily relied upon for four purposes in the digital realm: to provide data-based (ie, individualised or targeted) advertisements, to provide individualised services (eg, personalised search,

² For example, see Kiran Garimella and others, 'Political Discourse on Social Media: Echo Chambers, Gatekeepers, and the Price of Bipartisanship' (2018) The Web Conference 2018.

³ Reuben Binns and others, 'Measuring Third Party Tracker Power Across Web and Mobile' (2018) arXiv:1802.02507, 3, 9; Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem' (2018) ACM WebSci'18, 23, 29.

⁴ Sebastian Schelter and Jérôme Kunegis, 'Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers' (2016) Proceedings of the ICWSM 2016, 679, 679.

⁵ On this, see Joel Purra and Niklas Carlsson, 'Third-Party Tracking on the Web: A Swedish Perspective' (2016) IEEE 28, 28.

⁶ Arvind Narayanan, 'There Is No Such Thing as Anonymous Online Tracking' *Blog of the Center for Internet and Society* (28 July 2011) <<http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking>> accessed 13 July 2018; Jonathan Mayer, 'Tracking the Trackers: Where Everybody Knows Your Username' *Blog of the Center for Internet and Society* (11 October 2011) <<http://cyberlaw.stanford.edu/blog/2011/10/tracking-trackers-where-everybody-knows-your-username>> accessed 13 July 2018.

⁷ Balachander Krishnamurthy, Konstantin Naryshkin and Craig Wills, 'Privacy Leakage vs. Protection Measures: The Growing Disconnect' (May 2011) Proceedings of the Web 2.0 Security and Privacy Workshop 5.

individualised recommendations, match-making or personal training), to charge individualised prices (eg, price steering, price discrimination) and to sell data sets onward (data brokerage).⁸

The prevalence of third-party tracking in our modern ecosystem cannot be ignored. Illustrative is a recent study which analysed close to one million free apps used on mobile devices and found that over 90% of these contained a third-party tracker, with nearly 18% of apps containing over twenty different trackers.⁹ Another study, which focused on web-based tracking, found that most secure and unsecure websites have at least one known tracker present – while top websites (ie, the top-10k global websites that are most popular with users worldwide) contain at least one third-party tracker in 95% of cases and more than one tracker in 70% of cases.¹⁰ These trackers add to the information gathered directly by the first party operating the website or app.

Trackers may be described as branches of a tree, which in large numbers reach most corners of our online landscape. Interestingly, the roots of the tree exhibit a more limited spread. When following different trackers from the branch back to their root (that is, the company that ultimately owns these trackers), a handful of companies dominate the scene. Google has been reported to be the most prevalent of third-party trackers, followed by Facebook and Twitter. A recent web-based study found that Google's third-party tracking was present on 90% of top domains and over 70% across all website categories scrutinised, while Facebook was present on about 40% of all website categories scrutinised, followed by Twitter at 25%.¹¹ Local third-party trackers exist as well, but they are usually restricted to their country of origin.¹² The picture is similar for app-based trackers, where trackers belonging to Alphabet (Google's mother company) were present in 88.44% of the nearly one million analysed apps, while trackers that can be traced to Facebook were present in 42.55% of apps, followed by Twitter (33.88%), Verizon (26.27%), Microsoft (22.19%), LinkedIn (20.62%) and Amazon (17.91%).¹³ The recent Microsoft/LinkedIn merger¹⁴ increased these two's third-party tracking presence to a combined 42.81% on the apps covered in this particular study – thus overtaking Facebook by a slight margin.

⁸ Oliver Budzinski, 'Wettbewerbsregeln für das Digitale Zeitalter? Die Ökonomik personalisierter Daten, Verbraucherschutz und die 9. GWB-Novelle' (2017) 43 List Forum für Wirtschafts- und Finanzpolitik 221, 228-230; Damien Geradin and Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' *SSRN* (2013) 3 f <<https://ssrn.com/abstract=2216088>> accessed 3 August 2018; Final Report to the European Commission, 'Consumer Market Study on Online Market Segmentation through Personalised Pricing/Offers in the European Union' (June 2018); Daniel Trabucchi, Tommaso Buzanza and Elena Pellizzoni, 'Give Away Your Digital Services: Leveraging Big Data to Capture Value' (2017) 60 Research-Technology Management 43, 46 ff.

⁹ Binns and others (n 3), 'Mobile Ecosystem' 23, 25.

¹⁰ Purra and Carlsson (n 5) 29, 31.

¹¹ Purra and Carlsson (n 5) 31.

¹² Schelter and Kunegis (n 4) 681. This study was conducted before the *Microsoft/LinkedIn* merger.

¹³ Binns and others (n 3), 'Mobile Ecosystem' 23, 27 (Table 1).

¹⁴ See *Microsoft/LinkedIn* (Case M.8124) Commission Decision of 6 December 2016.

Accordingly, a handful of platforms, which have direct access to user information and occupy important market junctions, also engage in third-party tracking which enables them to harvest data beyond the horizon.

In what follows we consider possible implications third-party tracking may have on the competition dynamic. We explore two interlinked dimensions. First, we look at the market power implications of third-party tracking. In doing so, we reflect on the ability of ex ante merger review to appraise the significance of these tools following consolidation. Second, we consider the possible areas in which third-party tracking may trigger an ex post analysis due to an adverse impact on the consumer.

III. Market Power and Merger Control

Extensive data gathering and analysis in digital markets has the capacity to support the creation of market power.¹⁵ That may, in particular, be the case when dealing with the amalgamation of data from multiple sources. Wide-ranging third-party tracking, controlled by a single company, can reinforce the data advantage that certain tech companies are already benefitting from. When the tracker is a leading platform, third-party tracking may enable it to combine quality data from a variety of sources with information gathered directly on the platform.

The scope of third-party tracking should therefore play a role in the consideration of market power, market dynamics and barriers to entry and expansion. It should also affect the appraisal of proposed concentrations between trackers as well as between platforms and trackers. In the context of mergers, it is worth of note that market power could emerge on the data dimension even when the core markets where companies operate do not lead to a significant overlap. Possible harm, following a concentration, may emerge when the merged entity has the ability and incentive to engage in exploitation or exclusion, facilitated by its tracking capacity.

Exploitation may emerge from the increased asymmetry in information between user and provider. Users are often unaware of the volume and quality of data held by the merged platform and its ability to link various sources and infer the users' identity therefrom. Data concentration in a rich setting provided by third-party trackers could undermine users' privacy and autonomy (even when the user took steps to limit the availability of information). As a result, price and behavioural discrimination as well as other forms of manipulations may be more easily deployed.

Exclusion may affect potential or existing competitors who may not be able to reach the required volume and richness in data to effectively compete. It may be in the form of

¹⁵ European Data Protection Supervisor, 'Privacy and Competitiveness in the Age of Big Data' (March 2014) para 60. The OECD considers that market power in the digital realm may, amongst other things, enable dominant companies 'to supply products or services of reduced quality, to impose large amounts of advertising or even to collect, analyse or sell excessive data from consumers.' OECD, 'Big Data: Bringing Competition Policy to the Digital Era' DAF/COMP(2016)14 (27 October 2016) para 48.

input foreclosure (limited availability of data to other providers) or customer foreclosure (preventing other trackers from operating on the platform).¹⁶ Input foreclosure may also take the form of providing competitors with a data set that is less comprehensive or of a lower quality than the data set that the tracker has access to.¹⁷ Furthermore, the scope of data may provide the company with a detailed view of the market behaviour of competitors and the behaviour of competitors' customers—leading to a one-sided transparency that may give rise to concerns.

Since power obtained through the consolidation of data is not necessarily reflected by market shares, the appraisal of the true data advantage stemming from the combinations of third-party tracking capacities is challenging. As a result, these dimensions have attracted, to date, limited attention.

Take for example the *Microsoft/LinkedIn* merger, which—as we saw above—significantly increased the scope and range of data acquired through third-party tracking. The transaction had a distinct effect on the quality and scope of the data that the merged entity can gather as a third-party tracker. In its decision, the European Commission found that both parties were active in separate markets relying on large amounts of data about individuals and companies,¹⁸ yet it held that data concentration in the post-merger setting would not raise competition concerns. It highlighted that both parties would be subject to the new General Data Protection Regulation (GDPR), which might curtail data combination.¹⁹ And while market power may increase through data combination on a 'hypothetical market for the supply of this data',²⁰ due to the parties' market positions the Commission did not expect competitive harm to arise. On the other hand, the Commission noted that the merger may improve user experience and lead to product innovation.²¹

A similar approach to input foreclosure and data concentration may be found in the appraisal of the *Facebook/WhatsApp* merger. There, the Commission noted the significant number of market participants that collect user data alongside Facebook. Accordingly, it held that even if Facebook was to use WhatsApp's user data, this would not strengthen its position in advertising services.²² The Commission voiced its reluctance to delve deep into privacy-related issues, thus primarily focusing on possible foreclosure. With respect to the possible effect on privacy, it

¹⁶ European Commission, Guidelines on the assessment of non-horizontal mergers [2008] OJ C265/6, paras 29-77.

¹⁷ European Commission, Guidelines on the assessment of non-horizontal mergers [2008] OJ C265/6, para 33.

¹⁸ *Microsoft/LinkedIn* (Case M.8124) Commission Decision of 6 December 2016, paras 29-50, 57-69.

¹⁹ *Microsoft/LinkedIn* (Case M.8124) Commission Decision of 6 December 2016, para 178.

²⁰ *Microsoft/LinkedIn* (Case M.8124) Commission Decision of 6 December 2016, para 179.

²¹ *Microsoft/LinkedIn* (Case M.8124) Commission Decision of 6 December 2016, paras 165, 249.

²² *Facebook/WhatsApp* (Case COMP/M.7217) Commission Decision of 3 October 2014 [2014] OJ C417/4, paras 168-191. While Facebook refuted the possibility of automatically and reliably matching Facebook and WhatsApp user accounts during the merger proceedings, it later transpired that technologically this had already been possible before the transaction's notification. As a consequence, Facebook received a €110 million fine for providing incorrect or misleading information to the Commission during the merger review. Substantively, however, this had no impact on the clearance decision because the Commission had taken an 'even if' approach to automated matching. See *Facebook/WhatsApp* (Case COMP/M.8228) Commission Decision of 18 May 2017 [2017] OJ C286/6.

noted that ‘[a]ny 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.’²³ The combination of sets of personal data and the competitive advantage that may flow from such an ability received only limited attention, not least due to the merging parties indicating such synergy would not be possible.²⁴

Another illustrative example is the *Google/DoubleClick* merger. One aspect of the appraisal of this transaction focused on the merged entity’s ability to affect the privacy of its users. Antitrust scholars and some enforcers raised concerns in view of the potential threat that this merger could pose to privacy, holding that this was an issue that antitrust law could and should address.²⁵ The European Commission did not oppose this merger, and held that the merged entity would in any case need to abide by its users’ fundamental rights, notably privacy and data protection.²⁶ The Commission opined that ‘the merged entity, let alone DoubleClick alone, would not have access to unique, non-replicable data because the type of information collected by DoubleClick is relatively narrow in scope. Other companies active in online advertising have the ability to collect large amounts of more or less similar information that is potentially useful for advertisement targeting.’²⁷ Similarly, in the US, the FTC did not challenge the merger, holding that it would not have a negative impact on consumer privacy.²⁸ FTC Commissioner Pamela Jones Harbour dissented and pointed out that DoubleClick has ‘access to a wealth of aggregated data about user preferences and Internet behavior, based on its cookie-enabled tracking of users as they travel among websites, and would seem to have a strong incentive to use it.’²⁹ She noted that ‘[p]ost-merger, the combined Google/DoubleClick will become a “super-intermediator” with access to unparalleled data sources.’ She further held that it was not certain whether other companies could surmount the barrier to entry to behavioural advertising which consisted in ‘amass[ing] a dataset of the same scope and size.’³⁰

Might these decisions reflect an underestimation of the true (aggregated) data advantage? The developments in third-party tracking and the concentration of aggregated data at the hands of a few key players would suggest so. In an environment in which volume, velocity, verity and

²³ *Facebook/WhatsApp* (Case COMP/M.7217) Commission Decision of 3 October 2014 [2014] OJ C417/4, para 164.

²⁴ See *Facebook/WhatsApp* (Case COMP/M.8228) Commission Decision of 18 May 2017 [2017] OJ C286/6.

²⁵ Peter Swire, ‘Protecting Consumers: Privacy Matters in Antitrust Analysis’ (19 October 2007) <<https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/>> accessed 16 July 2018; Pamela Jones Harbour, ‘Dissenting Statement – In the Matter of Google/DoubleClick’ (File No 071-0170, 20 December 2007) 9ff.

²⁶ *Google/DoubleClick* (Case COMP/M.4731) Commission Decision of 11 March 2008 [2008] OJ C184/10, para 368.

²⁷ *Google/DoubleClick* (Case COMP/M.4731) Commission Decision of 11 March 2008 [2008] OJ C184/10, para 269.

²⁸ FTC, Statement of the Federal Trade Commission Concerning Google/DoubleClick (File No 071-0170, 20 December 2007) 2-3.

²⁹ Pamela Jones Harbour, ‘Dissenting Statement – In the Matter of Google/DoubleClick’ (File No 071-0170, 20 December 2007) 6, n 20 (emphasis in original omitted).

³⁰ Pamela Jones Harbour, ‘Dissenting Statement – In the Matter of Google/DoubleClick’ (File No 071-0170, 20 December 2007) 8.

veracity of data are key, the ability to amalgamate a range of sources directly and indirectly, via third-party tracking, would require increased attention, with the aim of reflecting its true impact.³¹

Some legislators have indeed taken steps to improve competition law's ability to explore these dimensions. Notable is the position in Germany, where the central role played by data has led to amendments of legislation, where § 18 para 3a of the German Competition Act now specifically deals with the assessment of market power in multi-sided platforms and network markets.³² It enables competition enforcers to take a number of factors into account when assessing market power in these particular markets, namely direct and indirect network effects, multi-homing and switching costs, economies of scale related to network effects, innovation-driven competitive pressure and, importantly, access to data that is relevant for competition.

Furthermore, the realisation that data concentration is often not reflected through turnover has led to amendments of merger notification thresholds. Austria and Germany both introduced an additional value-based notification threshold into their respective national merger laws in 2017. In Austria, mergers must now be notified if a transaction exceeds the value of €200 million and the parties engage in significant domestic activity.³³ In Germany, a transaction must now be notified if it exceeds the value of €400 million, in addition to significant domestic activity.³⁴ These new thresholds will enable enforcers to investigate mergers in which data – also personal user data gathered through third-party tracking – is key.

IV. Exploitation

The possibility for exploitation which is driven by the asymmetry of information and data collection has been in the public eye in recent years. From a competition enforcement perspective, this area is challenging as it depends on one's view as to the scope and role of competition enforcement.

³¹ Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (OUP 2016); Konstantina Bania, 'The Role of Consumer Data in the Enforcement of EU Competition Law' (2018) 14 *European Competition Journal* 38, 73.

³² § 18 para 3a German Competition Act, German Federal Law Gazette I 2005/2114 as last amended.

³³ § 9 para 4 Austrian Cartel Act, Austrian Federal Law Gazette I 2005/61 as last amended.

³⁴ § 35 para 1a German Competition Act, German Federal Law Gazette I 2005/2114 as last amended. See also the joint Austrian and German guidelines on the issue; Bundeskartellamt and Bundeswettbewerbsbehörde, *Guidance on Transaction Value Thresholds for Mandatory Pre-Merger Notification (Section 35 (1a) GWB and Section 9 (4) KartG)* (July 2018).

The question ‘Is privacy a competition problem?’ has given rise to heated debate in competition circles.³⁵ Some think it is.³⁶ Others disagree.³⁷ Similarly, the role of competition law in preventing price and behavioural discrimination, and in addressing the transfer of wealth between consumers and providers, have both led to lively debate.³⁸

To the extent that algorithmic discrimination, and subsequent exploitation which is driven by erosion of privacy setting and controls, are deemed to be relevant factors in the competition assessment, the presence of third-party tracking would likely play a role in the analysis of harm. This is so, since third-party tracking could amplify a tracker’s data gathering capacity, impact on data concentration, undermine users’ privacy and autonomy, and increase the provider’s ability to exploit or manipulate.

Let us briefly explore the debate using two dimensions – that of quality degradation, and that of excessive data collection.

Quality Degradation

Privacy protection as a dimension of quality has been suggested as a possible subject of competition intervention.³⁹ The argument that a reduction in privacy may ultimately affect the quality of a product has gained increased acceptance.⁴⁰ Only recently, the European Commission acknowledged that privacy-related questions ‘can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality.’⁴¹

³⁵ Allen P Grunes, ‘Another Look at Privacy’ (2013) 20 *George Mason L Rev* 1107, 1117 ff; Autorité de la concurrence and Bundeskartellamt, ‘Competition Law and Data’ (10 May 2016) 23. See also Ariel Ezrachi, ‘The Goals of EU Competition Law and the Digital Economy’ (BEUC Discussion Paper 2018); Marco Botta and Klaus Wiedemann, ‘EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy: Exploring the Terra Incognita’ Max Planck Institute for Innovation and Competition Research Paper No 18-08 (2018) 21 ff.

³⁶ European Data Protection Supervisor (n 15); Bundeskartellamt, ‘Preliminary Assessment in Facebook Proceeding: Facebook’s Collection and Use of Data from Third-Party Sources Is Abusive’ (19 December 2017) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html> accessed 29 August 2018; Francisco Costa-Cabral and Orla Lynskey, ‘Family Ties: The Intersection between Data Protection and Competition in EU Law’ (2017) 54 *CMLRev* 11.

³⁷ *Facebook/WhatsApp* (Case COMP/M.7217) Commission Decision of 3 October 2014 [2014] OJ C417/4, para 164; Maureen K Ohlhausen and Alexander P Okuliar, ‘Competition, Consumer Protection, and the Right [Approach] to Privacy’ (2015) 80 *Antitrust L J* 121.

³⁸ See Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016). For a pre-digital debate on wealth transfers and competition law, see Robert H Lande, ‘Wealth Transfers as the Original and Primary Concern of Antitrust: The Efficiency Interpretation Challenged’ (1982) 34 *Hastings L J* 65.

³⁹ Robert H Lande, ‘The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern’ (2008) 714 *FTC: Watch* 1; Natascha Just, ‘Governing Online Platforms: Competition Policy in Times of Platformization’ (2018) 42 *Telecommunications Policy* 386, 388; Maurice E Stucke, ‘Should We Be Concerned About Data-opolies?’ (2018) 2 *Georgetown L Tech Rev* 275, 287.

⁴⁰ Swire (n 25); Theodor Thanner, ‘Rethinking Competition Law for the Digital Economy’ 11 *Austrian Competition Journal* (2018) 79, 81.

⁴¹ European Commission, ‘Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions’ IP/16/4284 (6 December 2016).

Consumer preference in this area, however, is not so easily gauged. Competition enforcement will necessarily need to find a way to deal with what has become known as the privacy paradox:⁴² while consumers value privacy, they often do not (or cannot) act on this preference.⁴³ In addition, the perceived lock-in effect experienced by users means that they are usually not able to bypass certain prevalent digital service providers,⁴⁴ while so-called tracking walls require users to agree to third-party tracking before accessing a certain website or service.

The German Bundeskartellamt's ongoing *Facebook* investigation is noteworthy as it represents a first attempt at coming to terms with diluted privacy protection from a competition perspective. The Bundeskartellamt has voiced concerns that Facebook's terms of service regarding user data may constitute an abuse of a dominant position on the market for social networks – as they allow Facebook to extensively collect user data from outside its social network, ie as a third party.⁴⁵ According to the Bundeskartellamt, this data can then be amalgamated with the particular user's Facebook data – even if the user has blocked web tracking.⁴⁶ The President of the Bundeskartellamt, Mr Andreas Mundt, suggested that Facebook's practices 'violate mandatory European data protection principles.'⁴⁷ He challenged the assumption that Facebook users' consent to these practices – the extent of which is unknown to the vast majority of Facebook users – can be considered to be effective.⁴⁸

With its *Facebook* proceedings, the Bundeskartellamt is navigating uncharted waters. It will need to propose a theory of harm that links the data harvested through third-party tracking to a quality degradation that impinges upon consumer welfare. Its pending decision may have important repercussions on other competition authorities that are keen to look at possible data abuses, be it at the level of the European Union itself or in other EU Member States. It may also inform competition enforcement in other data-driven digital markets.

Excessive Data Collection

Another possible theory of harm may focus on the exploitative effects of third-party tracking, and whether it may amount to excessive data collection. Similar to the analysis of excessive prices, one could consider the application of Article 102(a) TFEU to excessive or unfair data

⁴² See, for instance, Patricia A Norberg, Daniel R Horne and David A Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors' (2007) 41 *Journal of Consumer Affairs* 100; Henner Gimpel, Dominikus Kleindienst and Daniela Waldmann, 'The Disclosure of Private Data: Measuring the Privacy Paradox in Digital Services' (2018) 3 *Electronic Markets* 165.

⁴³ On these lock-in effects, see Agustín Reyna, 'The Psychology of Privacy – What Role for BE in Antitrust Enforcement?' 30th *CLaSF Workshop* (Graz, 19 April 2018).

⁴⁴ Frank Pasquale, 'Privacy, Antitrust, and Power' (2013) 20 *George Mason L Rev* 1009, 1022.

⁴⁵ Bundeskartellamt, 'Bundeskartellamt Initiates Proceeding against Facebook on Suspicion of Having Abused Its Market Power by Infringing Data Protection Rules' (2 March 2016) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html> accessed 29 August 2018.

⁴⁶ Bundeskartellamt, 'Background Information on the Facebook Proceeding' (19 December 2017) <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6> accessed 29 August 2018.

⁴⁷ Bundeskartellamt, 'Preliminary Assessment' (n 36).

⁴⁸ Bundeskartellamt, 'Preliminary Assessment' (n 36).

collection. As data is often hailed as the ‘new currency’ of the digital age, such an analogy may not be too farfetched.⁴⁹

EU competition law may accommodate such an application where the criteria for excessive prices – namely the excessive nature of the price compared to the economic value of the product, and the unfair character of the price⁵⁰ – are fulfilled by excessive data gathering.⁵¹ One could focus on the monetary price of personalized data,⁵² more broadly consider the dimensions of morality, dignity and privacy,⁵³ and take into account the justification for excessive data collection. Furthermore, competition law enforcers could assess whether the privacy policies that third-party tracking relies on constitute unfair trading conditions within the meaning of Article 102(a) TFEU.⁵⁴

According to this approach, an excessive amount of data within the meaning of Article 102(a) TFEU could be found where users are made to pay an amount of data that greatly surpasses what they reasonably expect. Such an approach is not without complexity, nor controversy. For instance, it has been found that users generally overestimate the value of some platforms’ services, while underestimating the value of the personal data they divulge in return.⁵⁵ Absent credible benchmarks, competition enforcers could rely on other legal standards such as the Unfair Commercial Practices Directive,⁵⁶ the GDPR,⁵⁷ or the forthcoming ePrivacy Regulation, as possible yardsticks.⁵⁸ In many instances, users may not be aware to what extent third-party trackers are able to scoop up personal data related to them, and are therefore not informed about the extent of the counter-performance that a certain privacy policy requires from them. As companies in a dominant market position have a special responsibility not to ‘impair genuine undistorted competition’,⁵⁹ an online platform misleading or deceiving its users as to the extent of third-party tracking that its privacy policy provides for may well be

⁴⁹ Budzinski (n 8) 235; Stucke (n 39) 284.

⁵⁰ See Case 27/76 *United Brands* EU:C:1978:22, para 252. Recently, the Court has hinted that there may be other ways of establishing an excessive price; Case C-177/16, *Latvian Copyright Society* EU:C:2017:689, para 37.

⁵¹ European Data Protection Supervisor (n 15) 29; Bania (n 31) 63 ff.

⁵² For methods of calculating the value of personal data, see OECD, ‘Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value’ *OECD Digital Economy Papers* No 220 (2 April 2013); Gianclaudio Malgieri and Bart Custers, ‘Pricing Privacy – the Right to Know the Value of Your Personal Data’ (2018) 34 *Computer Law & Security Review* 289, 296 f.

⁵³ See also Wolfgang Kerber, ‘Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection’ 11 *J of Intellectual Property L & Practice* (2016) 856, 857; Gianclaudio Malgieri and Bart Custers, ‘Pricing Privacy – the Right to Know the Value of Your Personal Data’ (2018) 34 *Computer Law & Security Review* 289, 294.

⁵⁴ Insisting on privacy policies providing the ‘critical link’ in this respect, see Botta and Wiedemann (n 35) 58.

⁵⁵ On this phenomenon, see Nathan Newman, ‘The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google’ (2014) 40 *William Mitchell Law Review* 849, 857 ff; Giovanni Buttarelli, ‘Strange Bedfellows: Data Protection, Privacy, and Competition’ (2017) 34 *Computer and Internet Lawyer* 1, 3.

⁵⁶ Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) [2015] OJ L149/22.

⁵⁷ 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 (General Data Protection Regulation, GDPR) [2016] OJ L119/1; Bania (n 31) 67.

⁵⁸ Proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final.

⁵⁹ European Commission, Guidance on the Commission’s enforcement priorities in applying Article 82 of the Treaty to abusive exclusionary conduct by dominant undertakings [2009] OJ C45/7, para 1.

misrepresenting facts.⁶⁰ Based on precedent, the Court may also rely on the principles of proportionality and fairness to judge whether an excessive amount of data has been harvested.⁶¹

While the debate on excessive data collection and its status as a stand-alone abuse is far from closed, the above shows that EU competition may already possess both the tools and the incentive to apply Article 102 TFEU to third-party tracking by companies in a dominant market position.

V. Concluding Remarks

While third-party tracking can yield benefits that power our current online environment, it may also amplify concerns when dealing with data concentration and exploitation. The amalgamation of multi-sourced data, often with limited user awareness, has significant implications to our privacy, autonomy and welfare.

Commenting on the surge in data collection and the right to privacy, Tim Cook, Apple's chief executive, pointed out that 'the desire to put profits over privacy is nothing new.' His comments – directed at the crisis in data privacy – are also relevant for our discussion. He noted how 'our own information ... is being weaponised against us with military efficiency. Every day, billions of dollars change hands and countless decisions are made, on the bases of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesised, traded and sold. ... This is surveillance. These stockpiles of personal data serve only to enrich the companies that collect them. This should make us very uncomfortable. It should unsettle us.'⁶²

As we consider the implications of third-party tracking, we should not underestimate the rise of multi-sourced data pools, operated by data and analytic giants. The extent to which third-party tracking would affect antitrust scrutiny remains to be seen, but evident already is the power change it fosters. As third-party tracking takes place across markets, across platforms and across devices, we might be witnessing a rise in power over consumers even when, seemingly, market power relating to a specific antitrust market is not there (yet). Third-party tracking poses a potential threat to consumers' privacy and may give rise to exploitation. In addition, the enhanced data gathering capacity and data concentration may lead to foreclosure and barriers to expansion and entry.

⁶⁰ By Analogy, note Case C-457/10 P *AstraZeneca v Commission* EU:C:2012:770. See also Harri Kalimo and Klaudia Mejcher, 'The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace' (2017) 42 ELRev 210, 226 f.

⁶¹ On this, see Case 127/73 *BRT v SABAM* EU:C:1974:25, para 15; *GEMA statutes* (Case IV/29.971) Commission Decision 82/204/EEC of 4 December 1981 [1981] OJ L94/12, para 36; *Duales System Deutschland (DSD)* (Case COMP/34.493) Commission Decision of 20 April 2001 [2001] OJ L166/1, para 112. *DSD* was upheld on appeal, see Case T-151/01 *Duales System Deutschland* EU:T:2007:154; Case C-385/07 P *Duales System Deutschland* EU:C:2009:456.

⁶² Tim Cook, Keynote at the 40th International Conference on Data Protection and Privacy (Brussels, 24 October 2018) <<https://www.youtube.com/watch?v=kVhOLkIs20A>> accessed 24 October 2018.

As is often the case with data, the enforcement tool box goes beyond traditional competition law remedies. Central here is the ability to provide effective privacy protection to individuals. In Europe, of relevance are the GDPR and the envisaged ePrivacy Regulation, both of which offer additional privacy protection.

The principle of data minimisation now contained in Article 5(1)(c) GDPR provides that personal data needs to be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.’ That provision has the potential to limit the volume of data harvested through third-party tracking. Indeed, initial observations indicate that third-party cookies on news sites in Europe have declined by 22% since the GDPR entered into force in May 2018.⁶³ Other observations, however, indicate that a number of big trackers – amongst them Google – now scoop up more user data than before the entry into force of the GDPR.⁶⁴ The trend toward increased data concentration persists.

The new ePrivacy Regulation, if and when adopted, will likely supplement the current European privacy rules for online communications providers which includes email, apps, instant messaging, online advertising networks and the IoT (Internet of Things). Unlike the current ePrivacy Directive, it is expected to explicitly apply to tracking cookies.⁶⁵ Importantly, its effectiveness, like the GDPR, will be determined by users’ perception and activism. The proposed ePrivacy Regulation in its Article 8(1) relies on user consent in order to determine the legitimacy of many third-party tracking techniques. As it stands, the proposal does not ban third-party tracking as such,⁶⁶ but adopts the same rules on user consent as the GDPR. It would also introduce more privacy-friendly browser rules.⁶⁷

While of great value, the effectiveness of these instruments may be undermined by the privacy paradox. Furthermore, few users invest time and effort in reading and considering the implication of their consent. The majority offers consent with little hesitation, as it enables users to gain immediate access to desired websites and applications. Accordingly, the formalities of consent may provide a suboptimal mechanism. The stricter requirements for

⁶³ Timothy Libert, Lucas Graves and Rasmus Kleis Nielsen, ‘Changes in Third-Party Content on European News Websites after GDPR’ (August 2018) 1 <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf> accessed 23 August 2018.

⁶⁴ Björn Greif, ‘Study: Google Is the Biggest Beneficiary of the GDPR’ (10 October 2018) <<https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr>> accessed 11 October 2018.

⁶⁵ Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications [2002] OJ L201/37; Proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final, Recital 6. For the latest version of the proposal, see Interinstitutional File 2017/0003 (COD) (5 December 2017).

⁶⁶ Frederik J Zuiderveen Borgesius, Sanne Kruikemeier, Sophie C Boerman and Natali Helberger, ‘Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation’ [2017] 3 European Data Protection LRev 353, 353. For the view that the requirement of freely given consent precludes the use of tracking walls, see European Data Protection Board, ‘Statement of the EDPB on the Revision of the ePrivacy Regulation and Its Impact on the Protection of Individuals with Regard to the Privacy and Confidentiality of Their Communications’ (25 May 2018) 2.

⁶⁷ Proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final, arts 9(2), 10.

freely given consent in the GDPR and in the proposed ePrivacy Regulation may assist in enhancing the protection to European users.⁶⁸ Against these, one should note the use of new strategies⁶⁹ and the rapid developments of new technology which may enable the industry to bypass specific regulatory instruments and come up with new mechanisms and technologies to achieve similar goals. Looking beyond the EU, it will be of interest to see whether other jurisdictions come up with a similar protection mechanism, or favour a free market approach with limited regulation.

With the regulatory and consent limitations in mind, competition law could add an important layer of protection against exploitative third-party tracking. Competition enforcers display an increased awareness and concern over tracking and data collection. Notable are the fines that the European Commission recently imposed on suppliers that tracked the retail prices of their retailers in order to enforce resale price maintenance,⁷⁰ as well as the ongoing antitrust probe into Amazon's use of data on its merchants.⁷¹ This awareness is not limited to Europe: in Australia, there are ongoing data-related investigations into DoubleClick, for instance.⁷² And in the US, the data breach related to Google+ that has only recently become public knowledge was met by calls for involvement of the Federal Trade Commission and of European

⁶⁸ In particular, see 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 (General Data Protection Regulation, GDPR) [2016] OJ L119/1, art 7 and Recital 42; Proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final, art 9(1) referring to the GDPR for rules on consent. See also the discussion in Zuiderveen Borgesius, Kruikemeier, Boerman and Helberger (n 66) 360-361. Note comments by European Commissioner for Competition Margrethe Vestager expressing her view that as long as Facebook adheres to the new European privacy rules, an EU competition law case of the same sort 'cannot happen. Because the new privacy rules said that companies cannot take more data from you than what they need in order to provide you with the service.'; Jorge Valero, 'Vestager: "I'd like a Facebook that I pay, with full privacy"' EURACTIV.com (27 June 2018) <<https://www.euractiv.com/section/competition/interview/vestager-id-like-a-facebook-that-i-pay-with-full-privacy/>> accessed 27 August 2018. Also notable are recent comments from Apple CEO Tim Cook, who claimed that despite online service providers' assertions to the contrary, they did not actually need access to vast amounts of personal user data in order to provide their services. Karen Gilchrist, 'Apple's Tim Cook: "Don't believe" tech companies that say they need your data' CNBC (3 October 2018) <<https://www.msn.com/en-gb/news/techandscience/apples-tim-cook-dont-believe-tech-companies-that-say-they-need-your-data/ar-BBNRBLG?ocid=spartanntp>> accessed 3 October 2018. For the full interview, see <<https://www.youtube.com/watch?v=VD1cP8SK3Q0>> accessed 3 October 2018.

⁶⁹ There have also been recent reports that Google may have seized the opportunity that the GDPR presented in order to switch its status from data processor to data controller in many of its contracts with publishers – leading to concerns that it may be trying to extend its power over the user data that it gathers from publishers; Natasha Lomas, 'Google Accused of Using GDPR to Impose Unfair Terms on Publishers' *Tech Crunch* (1 May 2018) <<https://techcrunch.com/2018/05/01/google-accused-of-using-gdpr-to-impose-unfair-terms-on-publishers/?guccounter=1>> accessed 23 September 2018.

⁷⁰ *Asus* (Case AT.40465) Commission Decision of 24 July 2018; *Denon & Marantz* (Case AT. 40469) Commission Decision of 24 July 2018; *Philips* (Case AT. 40181) Commission Decision of 24 July 2018; *Pioneer* (Case AT. 40182) Commission Decision of 24 July 2018.

⁷¹ Margrethe Vestager, 'Press conference on Luxembourg McDonald's State Aid case – Q&A on Amazon' (19 September 2018) <<http://ec.europa.eu/avservices/video/player.cfm?ref=1160574>> accessed 21 September 2018; Sam Schechner and Valentina Pop, 'EU Starts Preliminary Probe into Amazon's Treatment of Merchants' *Wall Street Journal* (19 September 2018).

⁷² Concerns about Google tying access to its personal search data to its demand-side buying platform DoubleClick Bid Manager have resulted in an ongoing antitrust probe in Australia; see Darren Davidson, 'DoubleClick in Sights of ACCC for Abusing Market Position' *The Australian* (16 July 2018).

authorities.⁷³ More specifically on point is the ongoing *Facebook* investigation in Germany. It suggests that tracking which complies with data protection rules may be caught out under competition law.⁷⁴ A violation of data protection rules is not a prerequisite for the finding of an infringement under competition law, nor does such a violation automatically lead to a competition law infringement.⁷⁵

⁷³ Senator Richard Blumenthal, Tweet dated 10 October 2018, 21:14 (@SenBlumenthal); Douglas MacMillan and Robert McMillan, 'Google Exposed User Data, Feared Repercussions of Disclosing to Public' *Wall Street Journal* (8 October 2018).

⁷⁴ Noting that Facebook formally complied with data protection rules, see Heike Schweitzer, Justus Haucap, Wolfgang Kerber and Robert Welker, 'Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen: Endbericht' (29 August 2018) 16. On the *Facebook* investigation, see also above.

⁷⁵ Likewise, actions that are legal under the intellectual property laws are sometimes susceptible to antitrust scrutiny; see Case C-457/10 P *AstraZeneca v Commission* EU:C:2012:770.