Facebook's Anticompetitive Lean in Strategies

Dr Liza Lovdahl Gormsen* **& Dr Jose Tomas Llanos†**

Abstract

Facebook is under fire on several fronts and with good reason. Regulators strive to make sense of and address a plethora of seemingly unrelated issues that arise from the operation of its platform. These range from antitrust, privacy violations, dissemination of harmful content and speech, deception and polarisation to political manipulation. This paper identifies Facebook's unrestricted and excessive data collection as a unifying theme that requires immediate antitrust action. Once a privacy-oriented social network, Facebook soon mutated into a surveillance machine designed to hoover people's personal data to identify and understand people's interests, preferences and emotions and turn that knowledge into profit through the sale of targeted ads. Since people's innate preference for privacy stood in the way of Facebook's growth, Facebook resorted to privacy intrusions and deception to access as much user data as possible, thereby gaining market power. Currently, its overwhelming dominant position in the social media market means that no matter how much data Facebook extracts from users, how transparent its information about its data processing practices is and how many privacy scandals ensue from its reckless handling of data, users have nowhere else to go. This paper provides a course of action to correct this unacceptable anticompetitive outcome. The imposition of unfair commercial terms on consumers, the distortion of the competitive process through privacy violations and misleading practices, the squeezing of news publishers' traffic and foreclosure of actual and potential competitors by Facebook, can be stopped. A combination of data and consumer protection measures alone cannot stop Facebook's actions, but antitrust enforcement can be used to curb Facebook's ability to reinforce its data-driven abuse of its market power.

* Senior Research Fellow at the British Institute of International and Comparative Law. The author is extremely grateful to the Open Society Foundation for providing funding for this research. I am also tremendously appreciative to Jorge Padilla for comments and suggestions. Any mistakes, misunderstandings or omissions are those of the author alone.
† Research Assistant, British Institute of International and Comparative Law; Associate Lecturer in Competition Law, King's College London.

Table of Contents

Introduction

It is commonly argued that the lure of monopoly rents is what drives undertakings to compete and innovate to outperform their competitors. In the quest for monopoly rents, the attainment of a dominant and even a monopoly position by a firm that is the most attractive to consumers may be in some cases the competitive process' natural outcome. Accordingly, there is nothing inherently bad or wrong about Facebook's voiced plan for social network market domination.[1]

Dominance, however, must only be achieved, protected and strengthened within the boundaries of competition on the merits, which yields the largest benefits for consumers in terms of price, quality, choice and innovation. Facebook's entry into the social network market was a highly positive development, as it fulfilled an unsatisfied demand for a reliable, privacy-focused social networking platform. Its innovations led to the convergence of separate software applications such as search, instant messaging, media player, music streaming and photo sharing, thereby greatly enriching online social interactions and consequently promoting consumer welfare.

Regrettably, Facebook's obsession for growth later derived into a business model, described below in section I, that relies excessively on unlawful antitrust practices. The business model not only deprives consumers of the benefits of competition, but also gives rise to a plethora of concerns on different fronts. These include widespread privacy[2] violations, the deepening of information asymmetries through deception and a number of other 'negative externalities' such as the reinforcement of people's addictive tendencies, dissemination of harmful online content, misuse of data, political manipulation and polarisation. Upon close examination of Facebook's business model and its evolution over the years, it is possible to see that the imperative need for data, especially personal data,[3] is

---

[1] 'Mark Zuckerberg Spent Years Shouting "Domination!" at the End of Facebook Meetings' (*The Week*, 10 September 2018) <https://theweek.com/speedreads/795122/mark-zuckerberg-spent-years-shouting-domination-end-facebook-meetings>.

[2] Article 8 of the Charter of Fundamental Rights of the European Union enshrines the protection of personal data as an independent right. See Charter of Fundamental Rights of the European Union [2010] OJ C 83/02. Whilst the case law of the European Courts of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) has considered privacy to be at the core of data protection, these rights are not identical, as they differ inter alia in their scope and with regard to their permissible interferences. With regard to the scope of these rights, private life does not necessarily include all information on identified or identifiable persons, which is exactly what data protection law covers. In addition, data protection law imposes obligations relating to the processing of personal data on public authorities and private parties, as opposed to the right to privacy, which cannot be invoked directly against private parties. In turn, with regard to permissible interferences, personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or on some other legitimate basis laid down by law; if these conditions are met there is no interference with the right to data protection, although the collection, storage or disclosure of said data may still interfere with private life. Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222, 222 However, given the huge overlap between these two rights, the terms privacy and data protection are used interchangeably in this paper.

[3] Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. 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 (General Data Protection Regulation) OJ L119/1 2016 Article 4(1).

the unifying theme for all of the aforementioned issues. This unifying theme should be at the core of any discussion about what to do with Facebook and its overwhelming power.

The operation of network effects and data-driven externalities has enabled a 'virtuous cycle'[4] for Facebook under which it has built and developed proprietary data siloes that have given it overwhelming power and a competitive advantage on an unprecedented scale. Facebook's competitors in the social network and display advertising segments cannot match the scale of Facebook's datasets, for which reason their competitive performance is increasingly reduced, whilst Facebook's position is concomitantly reinforced. In addition, Facebook has strategically blocked access to data and has otherwise availed itself of valuable information to foreclose competitors and eliminate potential competitive threats. Facebook's access to and control over data troves have significantly reduced competition in a number of digital markets. Accordingly, seemingly unrelated issues such as the loss of privacy, deep information asymmetries, political manipulation, monopolisation and dissemination of harmful content are all symptoms of the same disease: a business model predicated upon financial gain and growth enabled by the collection and processing of data, most of which of highly intimate and sensitive nature, by any means, irrespective of consumers' preferences and at any cost.

Facebook's strategy to achieve a dominant position and the anticompetitive practices in which Facebook has engaged to protect and strengthen its dominance and market power are the focus of this article. However, given Facebook's data-driven business model, these competition concerns are intrinsically related with issues falling within the scope of fields of law other than antitrust, especially data protection and consumer protection law. Broadly, Facebook has systematically deceived and violated the data privacy of its users[5] to fuel network effects and trigger data-driven economies of scale, scope and speed, thereby developing a data-driven competitive advantage that no actual or potential competitor, including Google,[6] has been able to match. Based on that data advantage Facebook has impaired the competitive performance of competitors and otherwise squashed nascent competitive threats. Accordingly, a causal connection between data privacy violations and deception to access and process more data and the growth of Facebook's market power is identified. It is argued that any effort to restore competition in the market segments where Facebook is a powerful player requires stronger enforcement of the applicable data protection and consumer protection rules in order to limit the scope of Facebook's data advantage and enable the appearance of alternative business models. Reinforced data privacy and increased transparency leading to reinvigorated competition, in turn, are likely to mitigate the magnitude of some of the negative externalities described above, such as Facebook's political influence the misuse of which has compromised our democratic processes.

Structure

This article provides an important insight that should inform any intervention and/or regulatory proposals that may be put forward in respect of Facebook: attacking the disease, that is, Facebook's ability and incentive to collect and process data, is likely to be

[4] See Section I.C.3.

[5] Whereas users are those who *use* a service and consumers are those who *pay money* for a service, given that users pay to use Facebook and its related services with their personal data, users and consumers are used interchangeably in this article.

[6] See text accompanying footnote 92.

significantly more effective to address and correct its various harmful consequences, or symptoms, than ad hoc responses to such symptoms as they emerge,[7] as if repairing an airplane mid-flight. Moreover, the need for remedial action is growing at a dramatic pace, since nasty diseases tend to propagate quickly, and this one is no exception.[8]

This article is structured as follows. Section I contains an overview of Facebook's multisided, data-driven business model, identifying the main relevant product markets on which it is active. It explains that the operation of strong network effects and data-driven externalities created a 'virtuous cycle' for Facebook, which in combination with other factors entrenched its market power and enabled it to attain a dominant position in the market for social networking services.

Section II describes Facebook's strategy to achieve dominance, and the role that privacy violations and deception played in this endeavour. It explains that Facebook's initial privacy-driven approach was instrumental to convince consumers to switch from the then-leading social networking platform, MySpace. However, when Facebook's growth began to slow, it started to use the information derived from the tracking of its users' interactions with the platform to inform the design of its social network and fuel consumer engagement. Since data collection and mining as a tool to propel growth proved successful, Facebook suddenly acquired the incentive to gather as much user data as possible, but this incentive was contrary to its initial privacy protection commitment and users' voiced preference for online privacy. This section shows that Facebook deceived its users to access more data than they intended to disclose, and that its privacy-intrusive and deceptive conduct was decisive to the development of a data-driven competitive advantage that cemented its dominance.

Section III addresses the different ways in which Facebook has abused its dominant position. Shortly after becoming the undisputed leader in the social network market, Facebook felt comfortable to fully depart from its initial privacy protection promises and force consumers to agree to contractual terms enabling pervasive tracking across the Internet as a precondition to use its products and services. This action amounts to an exploitative abuse consisting of the imposition of unfair trading conditions on consumers – a violation of Article 102 (a) TFEU - since the terms entail a degradation of service quality and impair consumer choice. Moreover, Facebook continues deceiving and violating the data privacy rights of its users to reinforce its market power and distort competition, in contravention of Article 102(b) TFEU. In addition, after making news publishers dependent on Facebook's traffic referrals, Facebook adopted a number of measures that reduced traffic to their websites, and offered them a 'solution' that promoted Facebook's financial interests and impaired news publishers' competitive performance. Furthermore, Facebook has been particularly effective in killing nascent competitors, before they can pose a serious competitive threat. In particular, it has strategically denied a number of apps that had promising growth potential or were becoming popular access to indispensable data necessary to reach viable scale. As a result, none of those apps could remain in the market. Also, based on mobile usage trends inferred from data largely gathered on the basis of deception, Facebook has been able to identify apps and apps' specific features that are gaining traction. Knowledge of these trends gave Facebook the ability to make strategic decisions and guided its acquisition strategy. Specifically, Facebook

[7] Such as for example the do not track initiative or the US Honest Ads Act. See 'Do Not Track' (*Electronic Frontier Foundation*) <https://www.eff.org/issues/do-not-track>; 'Issue One – The Honest Ads Act' (*Issue One*) <https://www.issueone.org/honest-ads-act/>.

[8] See text accompanying footnote 40.

attempted to buy actual and potential competitors that were seen as a potential threat, and when the acquisition route failed, Facebook copied its acquisition targets' innovations, leveraging its user base to ensure its copycat versions' success. As a consequence of these exclusionary practices, Facebook has entrenched its dominance and greatly chilled incentives to compete and innovate, to the detriment of consumers.

Section IV puts forward a number of remedies and policy proposals that are required to restore competition in the social network and display advertising markets, to make competition enforcement better equipped to the dynamics of data-driven sectors, and to curb the concentration tendency in online segments. As significant negative impacts on important aspects of our society and people's lives have ensued from Facebook's market conduct and operations, Facebook has unintentionally made the case for intervention in and even regulation of the digital world more compelling.

Section V concludes that calls for intervention and regulation, however, are grounded in diverse and disparate issues ranging from antitrust, data privacy, consumer rights and online speech to the protection of the democratic process. As policymakers and regulators across the globe grapple with Facebook without identifying a common thread running through these issues, regulatory or otherwise responses are bound to be misguided and fragmented, and congruently ineffective. Thus, this paper concludes that the best way forward is to deal with Facebook's business model directly. Given the essential role of data in Facebook's business model, over the years Facebook has dramatically broadened the scope of its data collection and processing activities. Currently, not only does Facebook collect and process highly detailed personal information about its over 2.3 billion users[9] on Facebook, but also about users of its highly popular Instagram, WhatsApp and Messenger apps. In addition, it tracks the behaviour of Internet users on millions of independently owned websites and mobile apps that are members of the Facebook Audience Network or that use any of Facebook's products such as the Like button or Facebook Login. According to Facebook, as of April 2018 the Like button appeared on 8.4 million websites, the Share button on 931,000 websites covering 275 million webpages, and 2.2 million Facebook pixels were installed on websites globally.[10] The reach of Facebook's surveillance machine is astonishing, capturing what people read, view, shop for, do and even do not do online,[11] and for Android users, whom they talk to and exchange SMS with.[12] There is however a tension between Facebook's surveillance and users' preference for privacy.[13] To circumvent users' privacy preferences in order to gain access to more data, Facebook has over and over again resorted to data privacy violations and misleading and deceptive practices to conceal its privacy intrusions, deepen information asymmetries and nudge users into disclosing more personal data than they wish. Facebook's imperative need for

[9] See Form 10-K "Annual Report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934" for the fiscal year ending on 31 December 2018, filed by Facebook with the U.S. Securities and Exchange Commission, available at https://www.sec.gov/cgi-bin/browse-edgar?company=facebook&owner=exclude&action=getcompany

[10] Facebook, 'Response to Questions Asked during "Facebook: Transparency and Use of Consumer Data" Hearing, House of Representatives' (2018) 114 <https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf>.

[11] Casey Johnston, 'Facebook Is Tracking What You Don't Do on Facebook' (*Ars Technica*, 16 December 2013) <https://arstechnica.com/information-technology/2013/12/facebook-collects-conducts-research-on-status-updates-you-never-post/>.

[12] Tom Warren, 'Facebook Has Been Collecting Call History and SMS Data from Android Devices' (*The Verge*, 25 March 2018) <https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android>.

[13] See Section II.A.

data is what drives it to encroach upon users' data protection rights, reinforce information asymmetries and deceive consumers.

I. An Overview of Facebook's Multisided Platform and Market Power

A. General

Broadly speaking, Facebook is a social network, that is, a web-based service that allow individuals to build public or semi-public profiles featuring their personal information and to generally make connections or 'online friendships' with other users.[14] Social networks' users can exchange messages (one-to-one, one-to-group or one-to-many), share information (by posting pictures, videos or links), comment on posts and recommend friends, although a site does not have to include all of these features in order to qualify as a social network.[15]

Facebook is more than just a social networking platform. Indeed, Facebook is a multisided platform that serves four groups of customers by facilitating interactions between them, thereby solving a transaction-cost problem.[16] In particular, Facebook provides its social networking site to users (the 'user side') at no monetary price, but in exchange for their personal data. On Facebook, users create profiles and photo albums, post content on their friends' profiles, express their opinion on the posts of other users (for instance, by 'liking' or commenting thereon), disclose their activities or life events and engage in multiple other virtual social interactions. The more users, traffic and engagement exist in the platform, the more attractive and valuable the platform is to users. This user-generated content, which is organised and systematically updated by Facebook's popular features such as the newsfeed[17] and the timeline[18] 'constitutes a pool of data that is used to attract advertisers'[19] (the 'advertiser side'). In particular, Facebook serves this second group of customers by showing on their behalf, for a price, ads that are as-targeted-as-possible at each specific user.[20] Broadly, ads are targeted on the basis of users' preferences and interests that are inferred by analysing the personal information they enter on Facebook.[21] The more

[14] For a comprehensive description of social networks see Danah Boyd and Nicole Ellison, 'Social Network Sites: Definition, History, and Scholarship' (2007) 13 Journal of Computer-Mediated Communication 210.

[15] *Case COMP/M7217, Facebook/WhatsApp (2014)* para 51.

[16] See generally David S Evans and Richard Schmalensee, 'The Industrial Organization of Markets with Two-Sided Platforms', *in David S. Evans (ed), Platform Economics: Essays of Multi-Sided Businesses* (Competition Policy International 2011).

[17] The newsfeed is a regularly updating dynamic display of stories from friends, pages and other entities to which a user is connected. It includes posts, photos, event updates, group memberships, and other activities. Each user's newsfeed is personalised based on his or her interests and the sharing activity of his or her friends and connections. *Case COMP/M.7217, Facebook/WhatsApp (2014)* (n 15) para 154.

[18] The timeline allows users to organise and display the most important events and activities, enabling them to curate their memories in a searchable personal narrative that is organised chronologically. Users chose the information to share on their timeline, such as their interests, photos, education, work history, relationship status, and contact information, and users control with whom content is shared on their timeline. ibid 155.

[19] Florence Thépot, 'Market Power in Online Search and Social-Networking: A Matter of Two-Sided Markets' [2012] CLES Working Paper Series 4/2012 8 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2307009>.

[20] *Case COMP/M.7217, Facebook/WhatsApp (2014)* (n 15) para 70.

[21] Over time, Facebook has dramatically expanded the scope of its data collection operations. See text accompanying footnotes 9 and 10.

targeted the ad, the more likely that users act upon it, and therefore the higher advertisers' return on investment (ROI) is. Advertising on Facebook is broadly considered as display advertising, and can take different forms. For example, an advertiser can create a page for a brand it wants to advertise (for example, Adidas page), buy advertising space on Facebook's website or buy 'social ads'.[22] However, Facebook's advertising services are not limited to Facebook's social networking site. Over the years Facebook has expanded significantly its ecosystem by acquiring companies such as WhatsApp and Instagram, thereby broadening the web properties where its ads can be shown. In addition, since April 2014 Facebook offers the option to run advertising campaigns outside its web properties, that is, on 'thousands of high-quality websites and apps' that comprise Facebook's Audience Network.[23]

Moreover, Facebook provides news referral services, thereby connecting news publishers (the 'publisher side') with users. Media companies create Facebook pages and post news content directly onto Facebook, and the content is shown to users in accordance with their revealed preferences and the curation decisions made by Facebook's algorithms. Facebook may provide links that refer users to the news publishers' websites, or alternatively the news content is hosted on Facebook.

Facebook makes available a set of development tools and application programming interfaces ('APIs') that allow application developers to seamlessly integrate with Facebook to create social apps and websites that enable users to share their activities with friends on Facebook (the 'developer side'). Think of apps such as Academia.edu, Odeon, Spotify and Candy Crush Saga. Upon connection of these apps to Facebook, activities such as the books people are reading, the movies people want to watch, the songs they are listening to and the games they are playing are more prominently displayed throughout Facebook's timeline and newsfeed. These apps enhance the value users place on Facebook's social network and drive more user engagement. According to Facebook, there were approximately 1.8 million apps and 1.5 million app developers active on Facebook between February and April 2018.[24] At the same time, app developers are able to reach Facebook's vast user base and convert their attention into some type of benefit for their business (for example, to increase engagement with the app developer's products and services, drive consumer awareness or gain insights into user behaviour).

Following a data-driven, advertising-supported business model, Facebook does not charge, as mentioned, users a monetary fee for joining and using the platform nor does it pay users for their data. It derives the majority of its revenues from (targeted) advertising. In exchange for the free use of its social networking services, Facebook collects and processes personal data about its users to infer their interests and preferences and generally train and perfect its algorithms. Based on the insights derived from data processing, Facebook's algorithms can improve the relevance of social interactions and ad targeting, thereby making its products more attractive to both users and advertisers. The higher the volume and variety of data with which its algorithms are fed, the better, smarter and more accurate

[22] A social ad is an online ad that incorporates and displays user interactions along with the user's persona (picture and/or name) within the ad content. See Catherine Tucker and Alexander Marthews, 'Social Networks, Advertising, and Antitrust' (2011) 19 Geo. Mason L. Rev. 1211, 1212.
[23] 'Help Centre - What Is the Audience Network?' (*Facebook Business*) <https://www.facebook.com/business/help/788333711222886>.
[24] Facebook, 'Response to Questions Asked during "Facebook: Transparency and Use of Consumer Data" Hearing, House of Representatives' (n 10) 645.

they become.[25] In particular, the more personal data at its disposal, the more targeted Facebook's advertisements are, which means better ROI for advertisers and more advertising revenues for Facebook. The more users interact with Facebook' services (i.e. increased user engagement) and the higher the number of users' activities that Facebook can track and record, the greater the extent to which Facebook can improve its algorithms and consequently propel growth and drive more profits. This business model is only possible due to Facebook's dominance and it changed over time. The more dominant Facebook became then more it ignored users' privacy concerns.

Facebook's reach and pervasive, relentless and ubiquitous collection of data have translated into influence in a number of ways. Research by Facebook's data scientists has shown that Facebook has the power to alter its users' mood by just changing how many positive or negative posts it shows in their feeds.[26] Moreover, Facebook has the ability to increase voter registration by reminding users of upcoming registration deadlines,[27] and similarly can increase voter turnout by showing users that their friends are voting.[28] Critically, based on its surveillance infrastructure, Facebook has the power 'to track, target and segment people into audiences that are highly susceptible to manipulation'.[29] Misuse of this power by third parties enabled the exploitation of people's ideological biases to influence the 2016 US Presidential election and the UK EU Referendum. The incidents of online political advertising with deceptive information,[30] 'fake news' to promote a political agenda[31] and the unlawful access and mining of personal data of millions of Facebook

[25] Maurice Stucke and Allen Grunes, *Big Data and Competition Policy* (Oxford University Press 2016) 16–28.
[26] Adam DI Kramer, Jamie E Guillory and Jeffrey T Hancock, 'Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks' (2014) 111 Proceedings of the National Academy of Sciences 8788.
[27] Niraj Chokshi, 'Facebook Helped Drive a Voter Registration Surge, Election Officials Say' *The New York Times* (20 January 2018) <https://www.nytimes.com/2016/10/13/us/politics/facebook-helped-drive-a-voter-registration-surge-election-officials-say.html>.
[28] Robert M Bond and others, 'A 61-Million-Person Experiment in Social Influence and Political Mobilization' (2012) 489 Nature 295.
[29] Dipayan Ghosh and Ben Scott, 'Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet' (2018) 6 <https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/>.
[30] According to Facebook, an estimated 10 million people in the US saw the ads, which focused on 'divisive social and political messages across the ideological spectrum, touching on topics from LGBT matters to race issues to immigration to gun rights.' Many of these ads did not violate Facebook's content policies. Facebook, 'Hard Questions: Russian Ads Delivered to Congress | Facebook Newsroom' (2 October 2017) <https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress/>.
[31] Alicia Parlapiano and Jasmine C Lee, 'The Propaganda Tools Used by Russians to Influence the 2016 Election' *The New York Times* (16 February 2018) <https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html, https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html>; In many developing countries with populations new to both democracy and social media, fake stories can be more widely believed. And in some of these countries, Facebook even offers free smartphone data connections to basic public online services, some news sites and Facebook itself, but limits access to broader sources that could help debunk fake news. One such place is the Philippines, where a spokesman for its populist president, Rodrigo Duterte, shared on Facebook an image of a corpse of a young girl believed to have been raped and killed by a drug dealer. Fact checkers later revealed that the photo had come from Brazil. Despite the debunking, proponents of Mr. Duterte's bloody crackdown on reported drug dealers and addicts still cite the image in his defence. Paul Mozur and Mark Scott, 'Fake News in U.S. Election? Elsewhere, That's Nothing New' *The New York Times* (22 December 2017) <https://www.nytimes.com/2016/11/18/technology/fake-news-on-facebook-in-foreign-elections-thats-not-new.html>.

users by Cambridge Analytica[32] have shown the world that Facebook's excessive and almost unrestricted data collection and processing operations have created a surveillance machine which, when misused, is capable of compromising the integrity and proper functioning of liberal democracies. Facebook's imperative need for data enabled this threat to our political systems.

Facebook's products and services are designed to encourage consumers to spend more time on them, since more consumer engagement attracts more users, and consequently more app developers and advertisers. In turn, higher numbers of customers in these groups facilitate more interactions on or with the aid of Facebook's products and services, which leads to the generation of more data to train its algorithms, drive more profits and promote further growth. Based on data Facebook holds about its users, its algorithms show personalised content that is consistent with their revealed interests, in a move to maximise users' time spent on Facebook. Personalisation, however, tend to intensify and radicalise users' experience, can create 'filter bubbles' where users only see information related to their preferences, and can build 'echo chambers' where users' beliefs are reinforced by like-minded or even more extreme content.[33] Furthermore, the need for hosting 'engaging' content to elicit more interactions and consequently more data has led to the dissemination of harmful and/or inappropriate content on some of Facebook's products and services, including hate speech, extremist views and suicide-encouraging content. Devastating consequences have ensued from this phenomenon, such as the case of 14-year-old Molly Russell who recently committed suicide in 2017 after seeing graphic self-harm content on Instagram,[34] or the exacerbation of genocide in Myanmar resulting from posts on Facebook inciting violence against Muslims by the extremist group Ma Ba Tha.[35] The curbing of inflammatory speech and content lies in tension with Facebook's design, since Facebook 'relies on an algorithm that tends to promote the most provocative content',[36] in an effort to engender more traffic, data and growth. Moreover, Facebook's design and reward mechanisms have reinforced the addictive tendencies of some Internet users.[37] Research has shown that people suffering from conscientiousness, extraversion, neuroticism and (social, family and romantic) loneliness are particularly prone to develop a 'Facebook Addiction Disorder', that is, a compulsive use of Facebook that becomes excessive or motivated by purposes of mood alteration, causing negative consequences such as difficulties with time perception, time management capabilities, work, study habits and friendship.[38] Polarisation, the dissemination of harmful online content and hate

[32] Carole Cadwalladr, '"I Made Steve Bannon's Psychological Warfare Tool": Meet the Data War Whistleblower' *The Guardian* (18 March 2018) <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.
[33] House of Lords, 'Regulating in a Digital World' (2019) 28.
[34] Richard Adams, 'Social Media Urged to Take "moment to Reflect" after Girl's Death' *The Guardian* (30 January 2019) <https://www.theguardian.com/media/2019/jan/30/social-media-urged-to-take-moment-to-reflect-after-girls-death>.
[35] Max Fisher, 'Inside Facebook's Secret Rulebook for Global Political Speech' *The New York Times* (27 December 2018) <https://www.nytimes.com/2018/12/27/world/facebook-moderators.html>; Tom Miles, 'U.N. Investigators Cite Facebook Role in Myanmar Crisis' *Reuters* (12 March 2018) <https://uk.reuters.com/article/us-myanmar-rohingya-facebook-idUKKCN1GO2PN>.
[36] Fisher (n 35).
[37] Competition Commissioner Vestager has observed that, because Facebook is 'designed to give us a "kick" of satisfaction and reward, we stay longer, and that makes us available for the advertising that is the whole business idea behind it all.' Uffe Taudal, 'EU Commissioner Margrethe Vestager: Facebook is designed to create addiction – like tobacco and alcohol' (*Berlingske.dk*, 7 April 2018) <https://www.berlingske.dk/content/item/387227>.
[38] Roberta Biocati and others, 'Facebook Addiction: Onset Predictors' (2018) 7 Journal of Clinical Medicine 118.

speech, and the reinforcement of people's addictive tendencies are all consequences of Facebook's efforts to increase consumer engagement and consequently the volumes of data it can access. While these observations are not strictly related to antitrust, they show that efforts to gain market power through increases in consumer engagement and surveillance can lead to an unrestricted monopoly causing dire consequences and great influence on pivotal aspects of everyday life.

Facebook's business model and its harmful consequences are propagating quickly. Indeed, 'an industry of snooping on people's daily habits has spread and grown more intrusive', where firms collect precise location data from apps installed on mobile devices the users of which enable location services to access local news, weather and other information.[39] That data reveals people's travels with remarkable accuracy,[40] and in some cases is updated over than 14,000 times a day.[41] The data is sold or analysed to provide services to advertisers, retail outlets and even hedge funds seeking insights into consumer behaviour, and is collected based on the 'permission' users give when prompted with incomplete or misleading notices that fail to disclose the extent of the data collection or the purposes for which the data may be used. This industry justifies its practices on the basis that it allows app developers to make ad money, advertisers can show more relevant ads, and consumers get free services, whilst Facebook CEO Mark Zuckerberg for years has argued that 'Facebook needs to be free in order for the company to accomplish its mission of connecting the world.'[42] Unfortunately, nothing is free here. The loss of privacy and control over personal data, the monopolisation of online markets, the trend towards widespread disinformation and polarisation and interferences with the integrity of liberal democracies are amongst the hefty prices that consumers and our societies have been forced to pay. Limiting Facebook's ability and incentive to gather data has become a necessary measure to both obtain due reimbursement of such prices and halt the propagation of the surveillance capitalism [43] business model and its nefarious consequences.

B. Relevant Markets

The first question that arises when defining multisided markets is whether one should include both sides of the platform in the market definition or just one side.[44] To answer

[39] Jennifer Valentino-DeVries and others, 'Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret' *The New York Times* (10 December 2018) <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>.

[40] An investigation by the New York Times gave the following example: '[A data dot] leaves a house in upstate New York at 7 a.m. and travels to a middle school 14 miles away, staying until late afternoon each school day. Only one person makes that trip: Lisa Magrin, a 46-year-old math teacher. Her smartphone goes with her. An app on the device gathered her location information, which was then sold without her knowledge. It recorded her whereabouts as often as every two seconds, according to a database of more than a million phones in the New York area that was reviewed by The New York Times. While Ms. Magrin's identity was not disclosed in those records, The Times was able to easily connect her to that dot." 'ibid.

[41] ibid.

[42] Kurt Wagner, 'Mark Zuckerberg Explains Why an Ad-Free Facebook Isn't as Simple as It Sounds' (*Vox*, 20 February 2019) <https://www.vox.com/2019/2/20/18233640/mark-zuckerberg-explains-ad-free-facebook>.

[43] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books; Main edition 2019).

[44] David Evans and Michael Noel, 'The Analysis of Mergers that Involve Multi-sided Platform Businesses' (2008) 16

this question, a dual distinction of two-sided markets has been put forward:[45] on the one hand, there are transaction markets, characterised by the presence and observability of a transaction between two groups of platform users, where charging a per-transaction fee or a two-part tariff is possible.[46] In these markets all platforms serve the 'same two sides'.[47] This is the case of software platforms, where a direct transaction between software users and app developers can be observed. On the other hand, there are non-transaction markets, where there is no direct transaction between two different groups of customers, as in the case of advertising-supported platforms (like Google's and Facebook's user side and advertiser side).[48] According to Filistrucchi *et al.* '[w]hether one should define a single market or two interrelated markets depends on whether we are dealing with a two-sided transaction market or a two-sided non-transaction market'.[49] In non-transaction markets multiple relevant markets should be defined for each side of the platform, whereas in transaction markets only one market should be defined.[50]

This distinction and related policy recommendation is both sound and grounded in reality, since in transaction markets a platform is 'either on both sides of the market or on none'[51], whereas in non-transaction markets a platform can be in the relevant market on one side but not on the other. For example, a software platform such as Facebook Platform must be on both the developer side and user side or on neither side, since a transaction between a user and an app developer (i.e. downloading and installing the app) takes places within the Facebook ecosystem or does not take place on Facebook at all. Conversely, advertisement-supported media platforms can be on one side of the market but not on the other. Imagine a market definition where the analyst is trying to determine in which segments Facebook and Google compete. It is highly unlikely that users regard Google and Facebook as substitutes (since broadly speaking users resort to Google to find information on the Internet whist they use Facebook to interact online with their friends and acquaintances). Therefore, Google and Facebook would belong to separate markets with regard to the user side. On the other hand, it is at least theoretically possible that advertisers regard search and display advertising as substitutes, for which reason Google and Facebook could be included in a broad 'online advertising' market.

In view of the above, it is possible to tentatively define four relevant markets for Facebook's multisided platform. Firstly, a market for 'social networking services' or 'social network market', which encompasses the users' side. Secondly, a market for 'display advertising', which comprises the advertiser side. These two markets are the two sides of Facebook's non-transaction advertising-supported segment. Thirdly, a market for 'news

[45] Eric van Damme, Lapo Filistrucchi, Damien Geradin, Simone Keunen, Tobias Klein, Thomas Michielsen and John Wileur, 'Mergers in Two-Sided Markets – A Report to the NMa (2010)
[46] Lapo Filistrucchi and others, 'Market Definition in Two-Sided Markets: Theory and Practice' (2014) 10 Journal of Competition Law & Economics 293, 298.
[47] The platform has to be active on both sides of the platform. For instance, a payment card provider must be active on both the buyer and merchant sides at the same time to be able to consummate transactions. It is technically impossible to process a transaction by using platform A on the shopper side and platform B on the merchant side. Therefore, platforms in transaction markets only face competition from other platform providers which are also active in both sides of the platform.
[48] The distinction between transaction and non-transaction platforms is to some extent equivalent to Evans and Noel's distinction between '"symmetric' MSPs, which are defined as MSPs that serve coincident sides and 'asymmetric' MSPs which are defined as MSPs that do not have at least one side in common". See David Evans and Michael Noel, 'Defining Markets that Involve Multi-Sided Platform Businesses: An Empirical Framework with an Application to Google's Purchase of DoubleClick', (2007), 7
[49] Filistrucchi and others (n 46) 301.
[50] ibid 302.
[51] ibid 301.

referral services', which covers the publisher side.[52] And finally, the transaction market for the set of tools and APIs that constitute the Facebook Platform[53] (including users and app developers), which will be referred to as the 'Facebook Platform' market.

C. Facebook's Market Power and Dominant Position in the Social Network Market

The generation of network effects is one of multisided platforms' main features, including Facebook (1). In addition, the collection and processing of user data, which is the core activity that enables the provision of Facebook's services, elicits significant data-driven externalities (2). Facebook's ability to harness and benefit from these two types of externalities has led to a 'virtuous cycle' (3). On account of said virtuous cycle and other factors, Facebook holds a dominant position in the market for social networking services (4).

1. Network effects

Network effects (also known as network externalities or positive-feedback effects)[54] can be direct or indirect. Direct (or club) network effects arise where there is interaction between the users of a product, and having more users makes the product more useful and valuable for all users. This is the case of Facebook's users' side. The more users are on the network, the more attractive the network will be, since the audience with whom they can interact is larger. As a matter of fact, it is reported that every new Facebook user brings in 200 friends on average.[55] As a result, networks with a large use base tend to grow bigger, as they attract more users, all else being equal. Conversely, indirect network effects arise where the increasing use of a product increases its attractiveness to another economic group, which in turn renders indirect benefits for the original users of the product. This is the case of operating systems (OSs) and software platforms such as the Facebook Platform. Widespread adoption of Facebook attracts application developers, since they can access a larger audience to which they can offer their apps, and by devising and making available new applications compatible with Facebook's APIs, they increase Facebook's value for its users.

Network externalities may be positive for one group of customers but negative for another. A multisided platform creates value where one side benefits from more demand on the other side, even if the other side obtains no benefit or would even prefer less or no demand from the other side. This phenomenon can be seen in Facebook's advertiser side relative to the user side. Whereas advertisers place more value on Facebook the larger its audience is, users are likely to be indifferent or even annoyed by advertisements. Thus, Facebook enables the interaction between the two groups by subsidising users (with content or services), so they are willing to see advertisements. Insofar as the externalities' net value is

[52] The other side of this non-transaction market is the user side.
[53] See text accompanying footnote 152.
[54] With regard to network externalities in general see *e.g.* Stan J Liebowitz and Stephen E Margolis, 'Network Externality: An Uncommon Tragedy' (1994) 8 The Journal of Economic Perspectives 133, 130–150; Michael L Katz and Carl Shapiro, 'Technology Adoption in the Presence of Network Externalities' (1986) 94 Journal of political economy 822, 822–841; Michael L Katz and Carl Shapiro, 'Network Externalities, Competition, and Compatibility' (1985) 75 The American economic review 424, 424–440.
[55] House of Lords, 'Online Platforms and the Digital Single Market' 24.

positive, benefits arise from the interaction, some of which may be internalised by the platform.[56]

Indeed, the internalisation of network externalities is of the essence for a platform's success. The platform must recognise the interdependency between the demands from its different customer groups and devise a strategy to get enough customers on every side, so as to secure sufficient 'critical mass' and propel indirect network effects.[57] Without one side of the platform, the other sides will not join, and vice versa. This amounts to the well-known 'chicken and egg problem'[58] what side should join first? For instance, low or zero prices on one side aids the platform to solve the chicken and egg problem by attracting the participation of the benefitted group, which in turn, by propelling network effects, incentivises the participation of the non-benefitted group or groups (the so-called 'divide and conquer' strategy).[59] When a platform effectively manages to harness network effects and achieve critical mass, it is ready to take off and enjoy rapid growth.

On the contrary, a platform incapable of achieving critical mass is almost certainly doomed to extinction. If a platform does not achieve critical mass, the members who have joined it will tend to stop participating because the platform does not render enough value, and new members on the other side will stop joining because they cannot realise enough value either. In this case, instead of taking off, the platform implodes through reverse positive feedback effects: few customers on one side will cause a reduction in the number of costumers on the other side, which in turn leads to more customers on the first side exiting the platform, and so on. Needless to say, attaining critical mass is quite a challenging task which the immense majority of start-up platforms fail to accomplish.[60]

2. Data-driven Network Effects

The provision of Facebook's services relies on big data. Being a generic concept lacking a universally accepted definition, big data is commonly defined by reference to four 'Vs':[61] *volume* (large amounts of data), *velocity* (the speed at which data is generated, collected and processed), *variety* (the diversity of data coming from different sources) and *value* (the usefulness of the data for different purposes). Crucially, data's value derives from the insights it is possible to extract from analysing the data rather than from just amassing it.[62] The analysis of big data, performed through algorithms and advanced data processing techniques (i.e. big analytics), becomes more valuable to the extent that it allows for

---

[56] David S Evans and Richard Schmalensee, 'The Antitrust Analysis of Multi-Sided Platform Businesses' [2013] National Bureau of Economic Research Working Paper 18783 8 <http://www.nber.org/papers/w18783>.

[57] ibid 9.

[58] Bernard Caillaud and Bruno Jullien, 'Chicken and Egg: Competing Matchmakers' [2001] CEPR Discussion Paper No. 2885.

[59] Jullien, Bruno, 'Competition in multi-sided markets: divide and conquer' *American Economic Journal: Microeconomics* (2011) 186-219.

[60] For instance, by the time YouTube was commencing operations in 2005, there were over forty video sites attempting to secure enough viewers and take off, yet as of 2019 virtually all of such competing video sharing sites are gone. YouTube was the most successful video-sharing platform in obtaining both people uploading videos and viewers in enough numbers to ignite and attain exponential growth. David S Evans, 'The Web Economy, Two-Sided Markets and Competition Policy', in David S. Evans (ed), *Platform Economics: Essays on Multi-Sided Businesses* (Competition Policy International 2011).

[61] Christy Pettey, 'Gartner Says Solving "Big Data" Challenge Involves More Than Just Managing Volumes of Data' (*Gartner*, 2011) <http://www.gartner.com/newsroom/id/1731916>.

[62] Geoffrey A Manne and Ben Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework' (2015) 2 CPI Antitrust Chronicle 9.

specific patterns to be found and new correlations to be made between several datasets coming from combined different sources, as a result of which new information can be deduced or inferred, trends and behaviour can be accurately predicted and the likelihood for certain events to occur can be assessed with astonishing precision[63]. The more data is available for processing, irrespective of its apparent significance or value, the higher are the chances to obtain unexpected and potentially valuable information.[64]

Specifically, Facebook's collection and processing of users' personal data has enabled it to derive valuable information to personalise its services on the user side, improve ad targeting on the advertiser side and develop new technologies, thereby eliciting strong data-driven externalities.

Firstly, larger volumes of data lead to data-driven economies of scale. Based on the data gathered from user-generated content and users' interactions with the platform, Facebook's social network algorithms can increase the relevance of social network engagement, suggested friends or suggested interests that are shown to specific users. For example, the stories shown in a user's newsfeed are determined by the user's connections and activity on Facebook. In particular, Facebook shows more stories of the interest of a specific user that are posted by friends with whom such user interacts the most.[65] Similarly, Facebook targets ads based on the information it holds about users, be it age, gender, location, interests and any other inferred information, and the more information Facebook has, the higher the precision of ad targeting will be. As the Economist recently reported: '[t]he more users write comments, "like" posts and otherwise engage with Facebook, for example, the more it learns about those users and the better targeted the ads on newsfeeds become […] Facebook gets its users to train some of its algorithms, for instance when they upload and tag pictures of friends. This explains why its computers can now recognise hundreds of millions of people with 98% accuracy.'[66]

Secondly, greater variety of data leads to data-driven economies of scope. Linked data is a source of 'super-additive insights' and value that are greater than the sum of its isolated parts (data silos).[67] As Schepp and Wambach explain: '[t]he linkage of […] data [from different sources] can give companies more insights into user habits, enabling them to further improve their services and reinforce their market position. Generally speaking, the more data a company can combine, the better its chances to gain knowledge that can be used to strengthen its market position.'[68] For example, it has been reported that Facebook aims to create a digital assistant that has enough smarts to hold actual conversations with users on any topic.[69] Facebook can achieve this goal by resorting to data-driven economies of scale and scope. The more that users rely on Facebook's services (such as its social

[63] Primavera De Filippi, 'Big Data, Big Responsibilities' (2014) 3 Internet Policy Review 2.
[64] Directorate General for Internal Policies, 'Big Data and Smart Devices and Their Impact on Privacy' (2015) 11 <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf>.
[65] Facebook, 'Help Centre' <https://www.facebook.com/help/327131014036297/>.
[66] 'Data Is Giving Rise to a New Economy' (*The Economist*) <http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>.
[67] OECD, 'Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report' (2014) 29.
[68] Nils-Peter Schepp and Achim Wambach, 'On Big Data and Its Relevance for Market Power Assessment' (2015) 7 Journal of European Competition Law & Practice 120, 121.
[69] Richard Waters, 'Facebook Joins Amazon and Google in AI Chip Race' (*Financial Times*, 18 February 2019) <https://www.ft.com/content/1c2aab18-3337-11e9-bd3a-8b2a211d90d5>.

network platform, Messenger, Instagram or WhatsApp) and the greater the variety of personal data on particular users Facebook has, the better and smarter the digital assistant will be.

Thirdly, the velocity of data processing leads to economies of speed, that is, 'the capacity of a company to use the velocity at which a data set grows to discern trends well before others.'[70] If users' interests suddenly change as a consequence of a recent event, data-driven platforms need to react rapidly and adapt to the new scenario. Given its unparalleled audience, Facebook has first access to data about recent events, which enables it to update relevant content more quickly than competing social network platforms, thereby generating more traffic, more data and more consumer engagement. For example, within the first twelve hours of news that David Bowie had died, thirty-five million people had one hundred million interactions about Bowie's passing on Facebook.[71]

3. Interaction Between Traditional and Data-driven Network Effects: the 'Virtuous Cycle'

In Facebook's multisided market, big data and big analytics enhance the effects of 'traditional' network externalities. As noted above, direct network effects are observed in the user side. As Gebicka and Heinemann observe: 'there is the idea of "I will have a Facebook profile because everyone is on Facebook", which suggests facility and as such guarantees less effort, and in consequence attracts more and more people.'[72] In addition, a large user base attracts app developers, news publishers and advertisers, thereby eliciting indirect network effects. The larger the user side, the larger the audience that app developers, news publishers and advertisers have at their disposal to supply their apps, news and target their ads. At the same time, more user engagement attracts more users, and consequently more data to collect and process. Based on the data about users gathered from their engagement with Facebook, social network algorithms can engage in trial-and-error and thereby increase the relevance of users' social experience. A more personalised social experience enabled by data further attracts more users, which in turn attract larger numbers of app developers, news publishers and advertisers. In addition, Facebook offers APIs and tools to application developers so they can devise and integrate apps in the platform, thereby having direct access to Facebook's users. As a result, users can access more and more applications without leaving their Facebook page, which generates more user engagement, traffic and therefore data.

In turn, more data derived from Facebook's large user base enables more efficient, targeted and valuable advertising.[73] For example, Facebook's 'sponsored stories' are generated from the actions a user takes with an advertiser's business or app (for instance, when a user or 'fan' likes an advertiser's page), and conveyed to such user's contacts (friends) on their newsfeeds. These stories allow an advertiser to broaden its reach 'by allowing [its] fans to

[70] Daniel L Rubinfeld and Michal S Gal, 'Access Barriers to Big Data' (2017) 59 Ariz. L. Rev. 339, 353.
[71] Colin Stutz, 'David Bowie's Death Leads to 100 Million Facebook Interactions in First 12 Hours' (*Billboard*, 2016) <http://www.billboard.com/articles/columns/rock/6836601/david-bowie-death-100-million-facebook-interactions-12-hours>.
[72] Aleksandra Gebicka and Andreas Heinemann, 'Social Media & Competition Law' (2014) 37 World Competition 149, 160.
[73] Howard A Shelanski, 'Information, Innovation, and Competition Policy for the Internet' (2013) 161 University of Pennsylvania Law Review 1663, 1680.

help their friends discover [its] brand and connect with [its] campaign objectives.'[74] Sponsored stories may consist of *inter alia* page likes (such as 'Liza likes British Airways'), apps used or games played ('Liza played Glory of Rome') or check-in activities ('Liza is at Starbucks'), and include a picture of the ad and a link to the advertiser's Facebook page.[75] This is a particularly effective type of advertising. As sponsored stories take the form of user content, they tend to elicit a more positive reaction and engagement on the part of users. As noted by Facebook: '[w]hen people hear about your brand from their friends, they're twice as likely to engage.'[76] Accordingly, these social ads are reportedly more effective (obtain higher click-through-rates) than 'traditional' display ads.[77] In *Facebook/WhatsApp,* the European Commission (the Commission) noted that several respondents considered that other forms of non-search advertising are 'not as effective as advertising on social networking websites and notably on Facebook, due to Facebook's large and highly engaged audience and its ad targeting opportunities.'[78] This is consistent with Tucker and Marthews' findings: 'when advertisers target ads based on who is friends with whom, they can double the number of clicks, because advertisers can uncover consumers who may also be interested in their product.'[79] In addition, the launch of Facebook's Audience Network has enhanced the effectiveness of Facebook's advertising services even further. According to Facebook: 'in a Facebook ad campaign study, conversion rates were eight times higher amongst people who saw ads across Facebook, Instagram and Audience Network than people who only saw the ads on Facebook.'[80]

Moreover, its acquisitions of Instagram and WhatsApp dramatically expanded the scope of Facebook's data collection with the consequence that Facebook has at its disposal the largest amount of data relevant for social network interactions and the provision of display and social targeted ads. These acquisitions and the consequent expansion of Facebook's 'data advantage' have organically entrenched its position in the social networking and display advertising markets, opening up new routes to drive more user engagement and therefore profits.[81] Facebook's announced integration of WhatsApp, Messenger and Instagram, which so far have been offered as stand-alone and separate services, is bound to compound this trend, as it is likely to make it easier for Facebook to share data across them to improve its ad targeting capabilities.[82]

---

[74] Facebook, 'Sponsored Stories for Marketplace - Facebook' (*yumpu.com*, 2011) 2 <https://www.yumpu.com/en/document/view/27691723/sponsored-stories-for-marketplace-facebook>.

[75] ibid 9.

[76] ibid 2.

[77] See generally Catherine Tucker, 'Social Advertising: How Advertising That Explicitly Promotes Social Influence Can Backfire' [2016] SSRN paper <https://ssrn.com/abstract=1975897>.

[78] *Case COMP/M.7217, Facebook/WhatsApp (2014)* (n 15) para 77.

[79] Tucker and Marthews (n 22) 1225.

[80] 'Help Centre - What Is the Audience Network?' (n 23).

[81] For example, Facebook and Instagram ads now may include a 'click-to-Messenger' or 'click-to-WhatsApp' button, which opens a Messenger or WhatsApp conversation with the user upon clicking on or tapping the respective button within the ad, as the case may be. See 'Help Centre - How My Click-to-Messenger Ad Will Appear to People on Facebook, Instagram and Messenger' (*Facebook Business*) <https://www.facebook.com/business/help/1444950442185441>; 'Facebook Ads Can Now Link to Brands' WhatsApp Accounts' (*Marketing Land*, December 2017) <https://marketingland.com/facebook-ads-can-now-link-brands-whatsapp-accounts-230156>.

[82] It is also likely to make the main components of Facebook's conglomerate more difficult to break up and spin off, in case governments and/or regulators decide that is warranted. See Dave Lee, 'WhatsApp, Instagram and Messenger to "Merge"' (25 January 2019) <https://www.bbc.com/news/technology-47001460>.

Ultimately, the interaction between Facebook's traditional network effects and big data and big analytics leads to a 'virtuous cycle':[83] more users attract more users and generate more data; user data is used to train algorithms to improve users' social networking experience by making their social interactions more relevant to their interests. A larger user base, in turn, attracts app developers who want to reach more users with their apps and news publishers who want to reach more users with their news, and more app usage and more available news elicit more traffic and more data. At the same time, user data is used to create user profiles and derive valuable insights to better target advertisements, which in turn attracts more advertisers and therefore more revenues. More revenues enable Facebook to acquire firms that hold valuable datasets or may yield some type of data advantage,[84] as a result of which Facebook can gather and process more data to improve its social networking and advertising services, thereby attracting more users, app developers, news publishers and advertisers, in a positive feedback loop whereby Facebook grows bigger and bigger, and so does its market power.

4. Facebook's Dominant Position in the Social Network Market

Facebook holds a dominant position in the worldwide market for social networks at least since 2012, the year in which Facebook acquired Instagram, thus eliminating its most immediate competitive threat and triggering data-driven efficiencies. As of December 31 of that year, Facebook had 1.06 billion users, of whom 618 million used Facebook on a daily basis.[85] No other social network has ever come remotely close to a user base like that, and its number of users grow year after year, currently reaching over 2.3 billion. Facebook's dominant position is likely to be more entrenched in the EEA, since according to the Commission, Facebook's market shares are greater in the EEA than at worldwide level.[86] The *Bundeskartellamt* recently found that Facebook has a dominant position in the German market for social networks, with a market share over 95 percent of daily active users and over 80 percent of monthly active users.[87] No reliable market share data is available at EEA level; however, it is safe to assume that Facebook's EEA market share resembles its market share in Germany, and at any rate, is well above the 50% dominance threshold set by the CJEU in *Akzo*.

Small social network operators such as Elgg and Diaspora may be included in this market, but given the strength of direct network effects, the substitutability of Facebook with other social network providers is fundamentally limited. This is because, from the users' point of view, the main factors to consider when joining a social network are its size and the possibility to find the people with whom they want to interact online.

---

[83] 'And there is a virtuous cycle here: more data means better machine learning, which means better services and more users, which means more data.' Nick Srnicek, 'We Need to Nationalise Google, Facebook and Amazon. Here's Why' *The Guardian* (30 August 2017) <https://www.theguardian.com/commentisfree/2017/aug/30/nationalise-google-facebook-amazon-data-monopoly-platform-public-interest>.

[84] See text accompanying footnote 479.

[85] Form 10-K "Annual Report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934" for the fiscal year ending on 31 December 2012, filed by Facebook with the U.S. Securities and Exchange Commission, available at https://www.sec.gov/cgi-bin/browse-edgar?company=facebook&owner=exclude&action=getcompany

[86] *Case COMP/M.7217, Facebook/WhatsApp (2014)* (n 15) para 66.

[87] Bundeskartellamt, 'Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources' (7 February 2019) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>.

According to the *Bundeskartellamt*, '[p]rofessional networks such as LinkedIn and Xing, as well as messaging services such as WhatsApp and Snapchat or other social media such as YouTube or Twitter are not part of the [social network market, since e]ven though these services are in parts competitive substitutes for Facebook, from the users' perspective they serve a complementary need.'[88] Importantly, Instagram is considered Facebook's closest competitor[89] and could be included in the social network market. However, as it is owned by Facebook since 2012, it exerts no competitive pressure on Facebook; quite the contrary, it reinforces its market power through data-driven externalities. This fact confirms that Facebook has no meaningful competitors in the social network market,[90] and that its position of dominance is both entrenched and unassailable.

Barriers to entry are high. The strength of direct network effects and the absence of alternatives of a similar size cause consumer lock-in, which is reinforced by social pressure to have a Facebook account. As Weber Waller observes, '[w]hile temporary deactivation [of a Facebook account] is not particularly difficult, it can be psychologically and socially difficult, with friends, colleagues, and family members being unable to reach you through the system and inquiring off-line if everything is ok.'[91] Relatedly, the strength of Facebook's direct network effects is the most plausible explanation for Google's unsuccessful venture in the social network market. In 2011 Google launched its Google+ social network, which quickly became the 'fastest-growing network thingy ever', with more than 500 million users in just 18 months.[92] However, Google could not convince users to share content on and engage with its social network platform. Google+ could not overcome Facebook's direct network effects, because users wanted to share content where their *entire* group was, and they did not want to have a shared social network experience in a second redundant place. Congruently, the threat of potential competition does not seem to be a credible constraint disciplining Facebook. If Google, with its financial strength and big data advantage, was unsuccessful in its attempt to displace Facebook, it seems unlikely that other undertaking may succeed in doing so. Disruptive innovation from unexpected sources, as the Schumpeterians contend, is always a threat in high-tech markets, but if not supported by evidence and a dynamic record of entry, it is only speculation, and as such it should not be given too much weight.

Moreover, indirect network effects raise barriers to entry even further. Since advertisers want to reach as much 'eyeballs' as possible, they naturally choose the network having the largest user base. Competing platforms consequently need to reach critical mass to successfully enter the two-sided ad-funded social network market, but direct network effects stand in the way.

Last but not least, Facebook's virtuous cycle gives Facebook a data-driven competitive advantage that competitors cannot match. The data Facebook gathers from users'

---

[88] Bundeskartellamt, 'Background Information on the Facebook Proceeding' (2017) 3 <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.html>.

[89] Billy Cheung, 'Who Are Facebook's Main Competitors?' (*Investopedia*, May 2019) <https://www.investopedia.com/ask/answers/120314/who-are-facebooks-fb-main-competitors.asp>.

[90] This explains why when Zuckerberg was asked by US Senator Lindsey Graham to names services that consumers could use instead of Facebook, Zuckerberg could not do it. See Facebook Congressional Hearing Before the Committees on the Judiciary and Commerce, Science and Transportation, 115th Cong. (April 2018), https://www.youtube.com/watch?v=VbjC4uKXbvE

[91] Spencer Weber Waller, 'Antitrust and Social Networking' (2012) 90 NCL Rev. 1771, 18.

[92] Google, 'Google+: Communities and Photos' (*Official Google Blog*, 2012) <https://googleblog.blogspot.com/2012/12/google-communities-and-photos.html>.

interactions with its services, which is essential for product design and ad-targeting, is not available to actual and potential competitors in the volume, variety and velocity required to challenge Facebook.[93] Thus, this data advantage serves as an additional barrier to entry.

II. Facebook's Two-Stage Strategy to Achieve Dominance

It is commendable that Facebook has managed to grow into the ecosystem it currently is within no more than 15 years. How did this happen? As seen above, getting the necessary amount of consumers on every side of a platform is not an easy task.[94] Moreover, the collection and processing of user data, including personal data, is of the essence to the operation and improvement of Facebook's services. However, consumers have a long-standing preference for online privacy, and therefore dislike the collection of their personal data (A).

Faced with the challenge of reaching the necessary scale to 'take off' and become viable, and then constrained by consumers' revealed preference for online privacy, Facebook embarked upon a two-stage strategy. At first, Facebook entered the social network market as a provider with a strong privacy protection commitment. This commitment was decisive for Facebook's successful market entry and early expansion (B). However, as Facebook's growth began to slow down, Facebook made the decision to start carefully tracking its users' interactions with the platform and use the derived insights to make its social network more engaging. Data analytics to drive growth proved successful, and as Facebook progressively gained sufficient scale, it began rolling back on its privacy protection promises, concealing this 'change of heart' with deception.

In particular, Facebook issued a plethora of false and misleading statements and engaged in otherwise deceptive practices to conceal countless data privacy violations of its users aimed at increasing consumer engagement, traffic, growth and the volumes of data to which it could access to attain and strengthen a dominant position in the social network market, and ultimately improve its ad targeting technology to drive more profits. Crucially, Facebook's misleading and deceptive conduct ensured that its users would not switch due to its broken privacy promises, at a time where the social network market remained competitive. However, once Facebook became dominant in the social network market, Facebook was able to fully depart from its original privacy protection commitments without risking major consumer switching (C).

A. Consumers' Long-standing Preference for Online Privacy

The ability of consumers to browse and carry out activities online without being watched has been a salient concern since the early 2000s. A March 2000 BusinessWeek/Harris Poll showed that 86 percent of users wanted a web site to obtain opt-in consent before collecting users' names, address, phone number, or financial information. The same poll showed that 88 percent of users supported opt-in as the standard before a web site shares personal information with others.[95] Similarly, a 2001 survey conducted in the US found

[93] Jose Tomas Llanos, 'The Data Paradox in Competition Enforcement' [2018] TLI Think! Paper 10/2019 28 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3373553>.
[94] See Section I.C.1 and footnote 60.
[95] Electronic Privacy Information Center, 'EPIC - Public Opinion on Privacy' <https://epic.org/privacy/survey/>.

that 67 percent of Americans identified online privacy as a big concern.[96] In the same vein, a March 2000 BusinessWeek/Harris Poll found that 89 percent of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity. The same poll found that 63 percent of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally-identifiable information.[97] Also, an August 2000 study conducted by the Pew Internet and American Life Project found that 54 percent of Internet users objected to tracking, and a July 2000 USA Weekend Poll showed that 65 percent of respondents thought that tracking computer use was an invasion of privacy.

Recent survey data confirms the general and widespread concern about online data processing practices. According to a survey published in August 2018 by the UK Information Commissioner's Office, 53% of British adults are concerned about their 'online activity being tracked.' [98] Moreover, the European consumer protection organisation BEUC has reported that 70% of EU consumers are worried about how their data is being collected and processed.[99] Similarly, in a study commissioned by IAB Europe in which 11,000 people across the EU were surveyed about their attitudes regarding online media and advertising, it was reported that only '20% would be happy for their data to be shared with third parties for advertising purposes.' [100] In the same vein, the 2016 Eurobarometer survey of 26,526 people across the EU found that '[s]ix in ten (60%) respondents have already changed the privacy settings on their Internet browser and four in ten (40%) avoid certain websites because they are worried their online activities are monitored. Over one third (37%) use software that protects them from seeing online adverts and more than a quarter (27%) use software that prevents their online activities from being monitored'.[101] This is consistent with the 2011 Eurobarometer survey which found that disclosing personal data is a big issue for 63% of respondents at EU level, and for 67% of UK respondents.[102]

In the US, a study commissioned by TRUSTe found that '[…]consumer online privacy concerns remain extremely high with 92% of US internet users worrying about their privacy compared with 89% in January 2013. The high level of concern is further evidenced by 47% saying they were always or frequently concerned and 74% were more concerned than last year.'[103] Similarly, in a study on adults' perceptions about online advertising, 64% of respondents agreed to the statement 'someone keeping track of my activities online is

[96] John Schwartz, 'Giving Web a Memory Cost Its Users Privacy' *The New York Times* (4 September 2001) <https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html>.
[97] Electronic Privacy Information Center (n 95).
[98] Harris Interactive for the Information and Commissioner's Office, 'Information Rights Strategic Plan: Trust and Confidence' (2018) 21.
[99] BEUC, 'Supplementary Written Evidence (OPL0068) – Online Platforms and the EU Digital Single Market, BEUC Additional Comments" (2015) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online-platforms-and-the-eu-digital-single-market/written/25081.html>.
[100] IAB Europe, 'Europe Online: An Experience Driven by Advertising. Summary Results",' (2017) 7 <http://datadrivenadvertising.eu/wpcontent/uploads/2017/09/EuropeOnline_FINAL.pdf>.
[101] European Commission, 'Eurobarometer: E-Privacy (Eurobarometer 443)' (2016) 5, 36–7 <http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124),>.
[102] European Commission, '"Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union"' (2011) Tables section, 15.
[103] TRUSTe, '"Consumer Opinion and Business Impact. TRUSTe Research Report"' (2014) 3.

invasive.'[104] Lastly, the Pew Research Centre reported in 2015 that '76% of [US] adults say they are "not too confident" or "not at all confident" that records of their activity maintained by the online advertisers who place ads on the websites they visit will remain private and secure.'[105] Respondents were the least confident in the online advertising industry keeping personal data about them private than any other category of data processor, including social media platforms, search engines, and credit card companies. 50% of respondents said that no information should be shared with 'online advertisers.'[106]

As will be seen below, users' attitudes toward online privacy played a significant role in Facebook's successful market entry. However, soon thereafter, they became a hindrance to Facebook's growth that Facebook circumvented on the basis of deception and misleading practices.

B. Stage 1 – Strong Privacy Protection Commitment

At the time Facebook entered the social network market (2004), MySpace was the market leader. Indeed, by 2006 MySpace became the most visited website in the US, and the biggest US Internet companies at the time (Google, Yahoo and AOL) had all launched competing services in a bid to convince MySpace's over 108 million users to switch.[107] The market, however, had not reached the tipping point yet,[108] and MySpace's open design, which was increasingly blamed for sexual predation,[109] suicides[110] and other unfortunate incidents,[111] provided newcomers and competitors with an opportunity to launch a successful challenge against the theretofore incumbent.

Facebook fully embraced that opportunity. Whilst MySpace featured an open architecture where anybody could join, Facebook's network was closed,[112] as it required new users to use their real names and to validate their identities with a university ('.edu') email address. These privacy features made Facebook 'fundamentally different from just about everything

---

[104] Aleecia McDonald and Lorrie Faith Cranor, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (2016) SSRN Paper 22 <https://papers.ssrn.com/abstract=1989092>.
[105] Mary Madden and Lee Rainie, 'Americans' View about Data Collection and Security - Pew Research Center' (2015) 7 <http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacyand-Security-Attitudes-5.19.15_FINAL.pdf>.
[106] ibid 25.
[107] 'Hanging with the In-Crowd' [2006] *The Economist* <https://www.economist.com/business/2006/09/14/hanging-with-the-in-crowd>.
[108] In 2007 the market was highly competitive, with many social networks striving to displace MySpace, including LiveJournal, LunarStorm, AsianAvenue, Cyworld, Ryze, Fotolog, MiGente, BlackPlanet, Friendster, Skyblog, Xing, Hi5, Orkut, Dogster, Flickr, Mixi, Hyves, Yahoo 360, Bebo, Windows Live Spaces and Facebook. See Boyd and Ellison (n 14) 212.
[109] Susanna Schrobsdorff, 'Predator's Playground' (*Newsweek*, 26 January 2006) <https://www.newsweek.com/predators-playground-108471>.
[110] Jennifer Steinhauer, 'Verdict in MySpace Suicide Case' *The New York Times* (26 November 2008) <https://www.nytimes.com/2008/11/27/us/27myspace.html>.
[111] Noah Shachtman, 'Murder on MySpace' [2006] *Wired* <https://www.wired.com/2006/12/murderblog/>; WIRED Staff, 'MySpace Murder: An Epilogue' [2006] *Wired* <https://www.wired.com/2006/11/myspace-murder-an-epilogue/>.
[112] Facebook started allowing only participants with a university (.edu) email address. High school and corporate networks were subsequently allowed in 2005, and then in September 2006 Facebook was opened to the general public. However, '[t]he change to open signup did not mean that new users could easily access users in closed networks - gaining access to corporate networks still required the appropriate .com address, while gaining access to high school networks required administrator approval.' Boyd and Ellison (n 14) 218.

else that had come before on the Internet, including Friendster and MySpace.'[113] MySpace allowed users to choose between making their profiles accessible to either the 'public' or to 'Friends only'.[114] Facebook had privacy options that allowed users to determine exactly who could see their information (for example, current students, people in their class or only people in their residential house,[115] and later on 'No one', 'Friends', 'Friends-of-Friends' or a specific 'Network').[116] Moreover, whilst MySpace user profiles were by default publicly accessible to anyone,[117] Facebook user profiles could not be made public to all users.[118] In this way, Facebook addressed the mounting privacy concerns surrounding MySpace to offer a 'more exclusive, secure and trusting environment,'[119] representing itself as a secure, privacy-driven alternative social network.

Facebook embodied its commitment to privacy in a short, easy-to-read privacy policy, carefully drafted to elicit consumer trust.[120] Crucially, whilst explaining Facebook's data collection practices with a reasonable degree of detail, the privacy policy enshrined Facebook's commitment not to interfere with its users' privacy with the aid of tracking technology (i.e. cookies).[121] Facebook's privacy-centred approach, as disclosed in its privacy policy, was successful in wining user trust and causing consumer switching. Indeed, in 2007, at a time when the reputation of social networking sites was increasingly under fire as a consequence of disturbing incidents reported in the media,[122] Facebook surpassed MySpace in number of unique users per month.[123] This development was consistent with numerous studies revealing that Internet users were concerned with online privacy[124] and research showing that the trust of Facebook's users in Facebook was higher than the trust of MySpace's users in MySpace. For this reason Facebook's users 'disclosed significantly more identifying information such as real name, email address, and so forth, compared to MySpace.'[125]

C. Stage 2 – Deception and Privacy Violations

Facebook's superior level of privacy protection was instrumental to its successful market penetration. However, by 2007, Facebook's growth began to slow down. To reverse this

---

[113] David Kirkpatrick, *The Facebook Effect: The Inside Story of the Company That Is Connecting the World* (unknown edition, Simon & Schuster 2011) 31.
[114] Boyd and Ellison (n 14) 213.
[115] Kirkpatrick (n 113) 31.
[116] Danah Boyd and Eszter Hargittai, 'Facebook Privacy Settings: Who Cares?' (2010) 15 First Monday <https://firstmonday.org/ojs/index.php/fm/article/view/3086>.
[117] Danah Boyd, 'Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life', *David Buckingham, ed., The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning* (The MIT Press 2007) 6.
[118] Boyd and Ellison (n 14) 218.
[119] 'Hanging with the In-Crowd' (n 107).
[120] The privacy policy was under 1000 words long, and stressed Facebook's committment to privacy in its opening sentence: 'Because we want to demonstrate our committment to our users' privacy, we will disclose our information and privacy practices below.' Facebook, 'The Facebook Privacy Policy (2004)' <https://web.archive.org/web/20050107221705/http://www.thefacebook.com/policy.php>.
[121] 'We do not and will not use cookies to collect private information from any user.' ibid.
[122] See above text accompanying footnotes 109, 110 and 111.
[123] Devon Glenn, 'The History of Social Media from 1978 - 2012 [Infographic]' (16 February 2012) <https://www.adweek.com/digital/the-history-of-social-media-from-1978-2012-infographic/>.
[124] See Section II.A.
[125] C Dwyer, S Hiltz and K Passerini, 'Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace', *Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09 - 12 2007* (2007).

trend, Mark Zuckerberg created the 'growth team', which would use data analytics to increase consumer engagement. The growth team was entrusted with 'developing a deep understanding of user behaviour to re-engineer the site. They had a simple aim: more users and more of their time.'[126] Data analytics soon proved effective, as Facebook overtook MySpace within months.[127] Facebook reached 145 million users in 2008,[128] year in which MySpace's number of users began to rapidly decline.[129] Yet, Facebook's newly gained incentive to track user behaviour to improve its algorithms clashed with its original privacy-driven approach and users' privacy preferences. Data privacy violations and deception were the tools Facebook chose to access more data, propel growth and prevent consumer switching.

To understand Stage 2 of Facebook's strategy, an explanation of the mechanism through which online tracking takes place is in order (1). Then, Facebook's pattern of deceptive conduct to propel user growth, increase user engagement and collect and process larger volumes of data is presented. Initially, competitive pressure prevented Facebook from successfully implementing user tracking (2). However, as the social network market was becoming more and more concentrated, Facebook engaged in more deceptive conduct to collect additional personal data and track people for commercial purposes. Finally, after the majority of Facebook's competitors exited the social network market and Facebook's dominance was entrenched, Facebook openly backtracked on its promise not to track its users (3).

1. User Tracking

At the time Facebook initiated its shrouded data collection practices, online user tracking was mainly effected with the aid of cookies, which are small text files invisibly installed by websites in users' web browsers to remember users' preferences and prior actions on such websites, such as language settings, log-in passwords and items added to the shopping trolley. Crucially, cookies allow to determine users' online behaviour with remarkable precision.

When surfing the Internet, a user just types into his browser the URL of the website he wants to visit, and the page is loaded. However, a lot is going on behind the scenes, as the loading of the webpage involves several HTTP requests for content by the browser and responses from the servers of the visited webpage.[130] During these HTTP request/response interactions, the website's server can send and place a cookie on the user's computer, assigning a number (for example, 876876876) that will uniquely identify the web browser in said computer (the so-called 'cookie ID'). After being installed on the user's browser, the cookie is sent back in conjunction with the HTTP request in each subsequent request for content from the server that installed the cookie,[131] thereby providing the website with the user's cookie ID and other information about the user's

[126] Hannah Kuchler, 'How Facebook Grew Too Big to Handle' (*Financial Times*, 28 March 2019) <https://www.ft.com/content/be723754-501c-11e9-9c76-bf4a0ce37d49>.
[127] ibid.
[128] Ami Sedghi, 'Facebook: 10 Years of Social Networking, in Numbers' (*the Guardian*, February 2012) <http://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbers-statistics>.
[129] Emma Barnett, 'MySpace by Numbers: How It Compares to Its Rivals' (6 January 2011) <https://www.telegraph.co.uk/technology/myspace/8243403/MySpace-by-numbers-how-it-compares-to-its-rivals.html>.
[130] Arnold Roosendaal, 'Facebook Tracks and Traces Everyone: Like This!' (Social Science Research Network 2010) SSRN Scholarly Paper ID 1717563 5 <https://papers.ssrn.com/abstract=1717563.>.
[131] ibid.

browsing session that can be derived from the components of the HTTP request, such as the exact URL being visited (for instance https://www.theguardian.com/commentisfree/2019/jun/04/climate-change-world-war-iii-green-new-deal), the time of the visit, the user's IP address and geographic location and the user's device description. Consequently, with the aid of cookies, a website owner can determine that user 876876876 read on his MacBook air the article 'The climate crisis is our third world war. It needs a bold response' on Friday at 22:00 hours from London, UK.

With information of this type, of course, accurate user profiles valuable for advertising can be built over time. However, widespread online tracking of Internet users for commercial purposes cannot take place without coordination between online entities. This is because only the server from which a cookie is sent has access to that cookie,[132] and the cookie may be read only when the user in whose browser the cookie was installed sends an HTTP request to that server. So if for example the Guardian places a cookie on a user's browser, it may access and read that cookie, and therefore determine the user's browsing activities, only when the user is on theguardian.co.uk, but not when the same user is on theindependent.co.uk and any other websites. Coordination would be achieved through the placement of 'third party cookies', which requires that third parties be allowed to place content on a website[133] (normally a piece of HTML code). Then, when a user makes a HTTP request to the server of that website, another HTTP request for content is made to server of the third party, which delivers the content along with a cookie. This cookie is also sent back with the HTTP request in each later request for content from the third party server that installed it, and since the HTTP request always includes data on the referrer (that is, the website on which the third party content is displayed), third parties can determine with precision when a user visited a specific website.[134] The placement of third party cookies would ultimately be the route Facebook chose to backtrack on its privacy protection promises to drive more traffic and growth.

2. Deception and Privacy Violations: Beacon

In November 2007, as MySpace was progressively imploding and Facebook was gaining momentum, Facebook broke for the first time its promise not to track users across the Internet through the launch of its advertising solution 'Beacon', which was deceptively advertised as a feature to 'allow users to share information from other websites for distribution to their friends on Facebook.'[135] The harmful consequences to online privacy caused by Beacon were soon uncovered, provoking a user backlash which ultimately led to the demise of this product.

Beacon was launched with the participation of 44 websites, including *inter alia* Sony Online Entertainment, TripAdvisor, the New York Times and Blockbuster,[136] all of which had to install a piece of Facebook HTML code on their websites. If a user, for example, booked a flight on TripAdvisor or carried out any activity on a website using Beacon, the website would show the user a popup asking for permission to include the relevant activity (for

[132] ibid.
[133] ibid 3.
[134] ibid 5.
[135] Facebook Newsroom, 'Leading Websites Offer Facebook Beacon for Social Distribution' (6 November 2007) <https://newsroom.fb.com/news/2007/11/leading-websites-offer-facebook-beacon-for-social-distribution/>.
[136] ibid.

example, the flight booked on TripAdvisor) in his Facebook profile.[137] The popup contained a 'No, Thanks' option which would decline permission, but if the user did not click on it, Facebook would receive the information about the user's activity on the website and publish it on his Facebook profile as a 'social advertisement.' These publications were free advertisement for those websites using Beacon.[138]

However, whilst Facebook expressly asked for the consent of its users to share information about their browsing activities with Facebook, in practice Facebook did not require that consent to track its users' activities on the websites participating in Beacon. This was a direct consequence of Beacon's design. Since the websites using Beacon had installed a piece of Facebook HTML code, whenever a user visited one of those websites an HTTP request for content would be made to Facebook's servers, irrespective of whether or not the user provided his consent. As seen above, HTTP request/response interactions allow web servers to place cookies on users' browsers and read them during a later visit; therefore, Facebook was readily able to place and read cookies during users' visits to websites using Beacon, thereby effectively tracking the activities of users that had clicked on the option 'No, Thanks'.[139]

Facebook represented that it was only monitoring the activities of consenting users, and that it neither received nor collected any data about users that denied the permission to share their activity on Facebook.[140] Yet, research engineer Stefan Berteau conducted a series of experiments on Epicurious.com, a site participating in Beacon, finding that transmission of user data to Facebook took place despite the 'No, Thanks' option having been selected on the opt-out popup.[141]

Crucially, non-consenting users were not informed that data on their activities on websites participating in Beacon was being transmitted to Facebook, nor were they given the option to block the transmission of data. Indeed, Facebook's privacy policy in effect at the time did not provide any information on this practice,[142] nor were there any opt-outs in its privacy settings. Worst still, it was subsequently discovered that Facebook tracked activities from all users visiting websites participating in Beacon, including people who had never signed up with Facebook or who had deactivated their Facebook accounts.[143] Accordingly,

---

[137] 'Ok Here's At Least Part Of What Facebook Is Announcing On Tuesday: Project Beacon' (*TechCrunch*, November 2007) <http://social.techcrunch.com/2007/11/02/ok-heres-at-least-part-of-what-facebook-is-announcing-on-tuesday/>.

[138] Dina Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy' (2019) 16 Berkeley Business Law Journal 56.

[139] ibid 57.

[140] Interviewed by the New York Times in relation to Beacon's potential invasion into users' privacy, then-Facebook's vice president of marketing and operations Chamath Palihapitiya was asked "[i]f I buy tickets on Fandango, and decline to publish the purchase to my friends on Facebook, does Facebook still receive the information about my purchase?", to which he replied "Absolutely not. One of the things we are still trying to do is dispel a lot of misinformation that is being propagated unnecessarily." Brad Stone, 'Facebook Executive Discusses Beacon Brouhaha' (*Bits Blog*, 29 November 2007) <https://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha/>.

[141] Juan Carlos Perez, 'CA: Facebook's Beacon More Intrusive than Previously Thought' (*InfoWorld*, 30 November 2007) <https://www.infoworld.com/article/2648187/ca--facebook-s-beacon-more-intrusive-than-previously-thought.html>.

[142] See Facebook, 'Facebook Privacy Policy 2007' (12 September 2007) <http://web.archive.org/web/20070912083143/http://www.facebook.com/policy.php> Therefore, this privacy policy could not elicit user consent for online tracking off Facebook with the aid of cookies.

[143] Juan Carlos Perez, 'Beacon's User Tracking Extends beyond Facebook, CA Says' (*Computerworld*, 3 December 2007) <https://www.computerworld.com/article/2537951/beacon-s-user-tracking-extends-beyond-facebook--ca-says.html>.

Facebook resorted to deceptive practices and statements and violated the privacy of both Facebook and non-Facebook users to collect and process more data than legally and contractually entitled, with an aim to gain a competitive advantage.

After the findings above were made public, users immediately expressed their discontent and dissatisfaction through numerous channels.[144] As Srinivasan observes, 'Facebook was founded upon the qualitative promise of no surveillance outside of Facebook and users did not want this to change. Consumer resistance is early proof of consumers' preference for no surveillance.'[145]

At the time of the Beacon uproar, the social network market was still competitive. Indeed, although MySpace's popularity was declining, it still had more than double the number of Facebook users, and there were growing rumours about Google's desire to grow its social network Orkut.[146] Also, Twitter had been launched in 2006, quickly attaining 'an almost cult-like' status. 2007 saw the entry of new competitors like Tumblr and Friendfeed.[147] Fearing consumer switching, Facebook changed Beacon to be an opt-in system, and soon thereafter released a privacy control to turn off Beacon completely.[148] However, Beacon's reputation was already tainted beyond repair, and in agreeing to settle a class-action lawsuit, Facebook decided to shut Beacon down in 2009.[149]

Zuckerberg apologised profusely for the privacy disaster arising from Beacon, calling it a 'mistake'.[150] Also, Facebook implemented a democratic process for future privacy policy changes[151] to assure its users that it would not collect their data and invade their privacy without meaningful consent, in a move to control the reputational damage and regain user trust. Time would later prove those apologies and measures insincere and empty.

---

[144] For example, a petition from MoveOn.org Civic Action quickly won the support of 50,000 Facebook users. Louise Story, 'The Evolution of Facebook's Beacon' (*Bits Blog*, 29 November 2007) <https://bits.blogs.nytimes.com/2007/11/29/the-evolution-of-facebooks-beacon/>; Also, there were countless articles online giving users instructions to block Facebook's beacon. See for example Kevin Purdy, 'Block Facebook's Beacon Feature' (*Lifehacker*, 6 December 2007) <https://lifehacker.com/block-facebooks-beacon-feature-330651>; Beacon even led to a class-action lawsuit against Facebook, claiming that Beacon was forced upon members, was not properly explained, and was too hard to opt out of. In an effort to resolve the lawsuit, Facebook offered to shut down Beacon and donate $9.5 to a foundation dedicated to exploring the issues around online privacy and security. The Telegraph, 'Facebook Shuts down Beacon' (21 September 2009) <https://www.telegraph.co.uk/technology/facebook/6214370/Facebook-shuts-down-Beacon.html>.

[145] Srinivasan (n 138) 59.

[146] Julie Sloane, 'Facebook Got Its $15 Billion Valuation — Now What?' [2007] *Wired* <https://www.wired.com/2007/10/facebook-future/>.

[147] Christopher McFadden, 'A Chronological History of Social Media' (*Interesting Engineering*, 16 October 2018) <https://interestingengineering.com/a-chronological-history-of-social-media>.

[148] Mark Zuckerberg, 'Thoughts on Beacon' (*The Facebook Blog*, 5 December 2007) <https://web.archive.org/web/20080107025500/http://blog.facebook.com/blog.php?post=7584397130>.

[149] Cade Metz, 'Facebook Turns out Light on Beacon' (23 September 2009) <https://www.theregister.co.uk/2009/09/23/facebook_beacon_dies/>.

[150] Zuckerberg (n 148).

[151] Facebook included in its Governing Documents a democratic process under which users were allowed to vote on future amendments to contractual documents that effected changes to users' privacy. See 'Facebook Drafts New Governing Documents, Adopts New User Voting Process on Policy Changes' (26 February 2009) <https://www.adweek.com/digital/facebook-drafts-new-governing-documents-process-for-user-voting-on-policy-changes/>.

3. More Deception and Privacy Violations: the Open Graph, the Graph API and Social Plugins

In Facebook's annual F8 conference held in May 2007, Facebook announced 'Facebook Platform', a feature that allowed app developers to build applications with deep integration into Facebook. 'Until now, social networks have been closed platforms. Today, we're going to end that', claimed Zuckerberg in the conference.[152] Apps would have 'granular privacy controls,' and Facebook users were free to decide which applications to add to their accounts, their order of appearance within their profiles, and when to remove them. Apps could be anything from a video sharing interface, a news publisher, a TV broadcaster, a job search interface, a music player to an online game.[153] These apps would gain distribution through the 'social graph', which is the 'network of real connections through which people communicate and share information' on Facebook.[154] For example, a user's friend adding an app could lead to a notification in the user's News Feed.[155] Zuckerberg told the conference:

'The social graph is our base, and we've built a framework that is completely optimized for developing social applications within our environment […] [w]e believe that there is more value for everyone in letting other people develop applications on top of the base we've built than we could ever possibly provide on our own.'[156]

On its face, the launch of Facebook Platform was a positive development. Facebook was effectively creating a market in its own right, enabling valuable interactions between two different groups of customers that would not meet but for the intermediary function of Facebook: users could access a number of additional services and features of their preference within Facebook, and apps developers could access Facebook's large user base to market their products. Consumer welfare was increased, as users enjoyed a greater variety of functionalities, and app developers had an incentive to engage in innovation and spur technological progress, thereby promoting dynamic efficiency.

However, Facebook Platform was intrusive by design. When a user installed an application, by default that application would query the Facebook API to gain access to all information on Facebook that the user could enter or see,[157] and since the app received the privileges

---

[152] Facebook Newsroom, 'Facebook Unveils Platform for Developers of Social Applications' (24 May 2007) <https://newsroom.fb.com/news/2007/05/facebook-unveils-platform-for-developers-of-social-applications/>.

[153] See for example Kristen Nicole, 'Facebook Platform: 30+ Awesome Applications for Facebook' (*Mashable*, 24 May 2007) <https://mashable.com/2007/05/24/facebook-platform-30-apps/>.

[154] Facebook Newsroom, 'Facebook Unveils Platform for Developers of Social Applications' (n 152).

[155] ibid.

[156] ibid.

[157] According to Facebook, 'Examples of the types of information that applications and websites may have access to include the following information, to the extent visible on Facebook: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, your relationship status, your dating interests, your relationship interests, your network affiliations, your education history, your work history, your course information, copies of photos in your photo albums, metadata associated with your photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall, a list of user IDs mapped to your friends, your social timeline, notifications that you have received from other applications, and events associated with your profile.' Facebook, About Platform, quoted in EPIC, 'In the Matter of Facebook, Inc., Complaint, Request for

of the profile owner, it could also access personal information about the user's friends.[158] Access to detailed personal data about users and their connections was a strong incentive for application developers to devise Facebook apps. Within one year since the launch of Facebook Platform, around 24,000 apps were built by 400,000 developers, and over 95% of Facebook users had installed at least one application.[159] Facebook benefited to a great extent from the proliferation of apps. Popular apps are 'a big Facebook traffic draw',[160] and since apps are integrated into Facebook, all app-related traffic takes place *within* Facebook. In turn, more traffic translates into more data that can be used for product development, ad targeting or other purposes.

Privacy concerns arising from Facebook Platform were soon covered in the media,[161] and given that Facebook was still dealing with the uproar ensuing from Beacon, in November 2009 it updated its privacy settings and privacy policy, announcing that it was giving 'you more control of your information […] and [had] added the ability to set privacy on everything you share.'[162] However, this update was extremely resisted and controversial,[163] ultimately leading in 2011 to a complaint against Facebook by the US Federal Trade Commission ('FTC') on the grounds that it had deceived consumers by failing to its keep privacy promises.[164]

The privacy concerns arising from Facebook Platform and the 2009 update of Facebook's privacy settings and privacy policy were compounded by Facebook's implementation of its goal to build 'a web where the default is social' proclaimed in the 2010 F8 conference.[165]

In that instance, Facebook announced the Open Graph and Social Plugins, which included 'Like' buttons on websites outside Facebook and auto-login capabilities for those websites. Broadly, Facebook redesigned its Facebook API (now called 'Graph API') for developers so that, in addition to being able to see the social connections between Facebook users, they could also see and create the connections people have with their interests, such as places, brands and other websites (the so-called 'Open Graph').[166] This would be achieved with the aid of 'Like' buttons across the Internet, and would enable developers to create subsets of the Open Graph around interests and things. For example, anytime a user would like a movie, song or restaurant on any website featuring a 'Like' button, that information would be sent back to Facebook, into the Open Graph. Accordingly, 'Yelp [would] know

---

Investigation, Injunction and Other Relief'
<https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf>.

158 F Adrienne and E David, 'Privacy Protection for Social Networking APIs', *The Web 2.0 Security and Privacy 2008 (in conjunction with 2008 IEEE Symposium on Security and Privacy)* (2008).

159 Kim Hart, 'A Flashy Facebook Page, at a Cost to Privacy' (12 June 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html>.

160 Caroline McCarthy, 'Understanding What Facebook Apps Really Know (FAQ)' (*CNET*, 25 October 2010) <https://www.cnet.com/news/understanding-what-facebook-apps-really-know-faq/>; See also Emily Steel and Geoffrey A Fowler, 'Facebook in Privacy Breach' *Wall Street Journal* (18 October 2010) <https://www.wsj.com/articles/SB10001424052702304772804575558484075236968>'Apps are considered an important way for Facebook to extend the usefulness of its network. The company says 70% of users use apps each month'.

161 Hart (n 159).

162 Facebook November 2009 Privacy Announcement, quoted in EPIC (n 157).

163 Many groups were created on Facebook opposing the new privacy settings, with names such as 'Against the New Facebook Privacy Settings!', 'Facebook! Fix the Privacy Settings" and 'Petition: Facebook, stop invading my privacy!'. See ibid 16–17.

164 FTC, 'In the Matter of Facebook, Inc., Complaint'.

165 Eric Schonfeld, 'Zuckerberg: "We Are Building A Web Where The Default Is Social"' (*TechCrunch*, April 2010) <http://social.techcrunch.com/2010/04/21/zuckerbergs-buildin-web-default-social/>.

166 ibid.

what restaurants you and your friends have liked elsewhere and take that into consideration when giving you recommendations, or Pandora with music, and so on.' [167] As a consequence, app developers would be able to access even more personal data about Facebook users.

Had Facebook duly informed its users about the privacy implications of installing Facebook apps and using Social Plugins, these products would have been lawful innovations designed to boost growth and traffic. However, the design of both Facebook Platform and Social Plugins was inconsistent with its users' privacy expectations and preferences, so Facebook resorted to deception again to conceal the intrusions of privacy enabled by the use of these products, ensure their widespread adoption and retain user trust.

For installation and operation, each app requests a number of *permissions* from the user installing the app, which confer upon the app the ability to access and collect rich information about that user. In particular, Facebook provides an 'access token' upon user's approval (steps 1 to 4 in Figure below), after which the app is able to collect the user's personal data in accordance with the relevant permissions given and store it in servers outside Facebook's ecosystem and users' control (steps 5 to 6 in Figure below).[168]

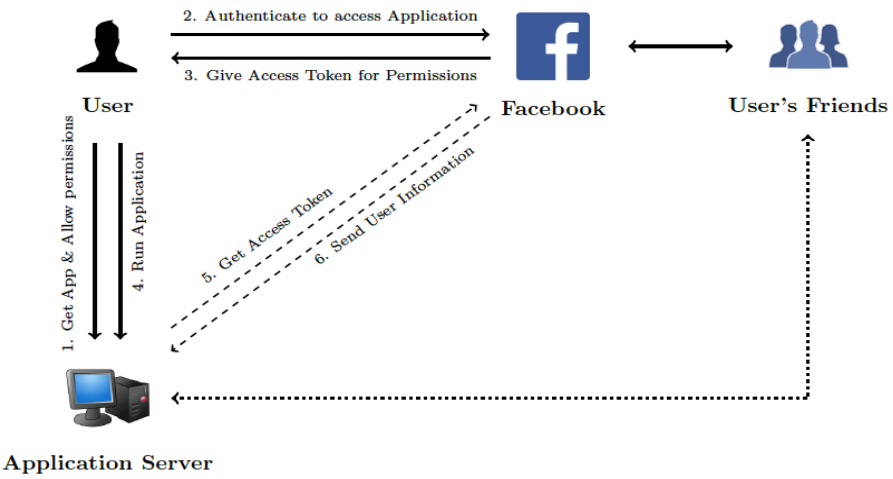

Figure 1: Facebook Applications Architecture Overview[169]

As indicated above, this mechanism was problematic because it was not duly disclosed that it enabled a permanent transmission of Facebook users' personal data to apps that had not been installed by them. In concrete, the transmission was concealed under privacy settings that were, in principle, especially designed to enable Facebook users to control 'who can see' their personal data.[170] In these privacy settings users could restrict access to different categories of personal data (for example, profile, personal info, photos, videos and employment information) to specified users, such as 'friends' and 'friends of friends.'[171]

[167] ibid.
[168] Iraklis Symeonidis and others, 'Collateral Damage of Facebook Apps: An Enhanced Privacy Scoring Model' 4 <https://pdfs.semanticscholar.org/3c7e/27bd24cbe2651fedfbee7bd73e858a4fd5b6.pdf>.
[169] ibid.
[170] FTC (n 164) para 11.
[171] Also, Facebook's Central Privacy Page and Profile Privacy Page then in effect expressly confirmed that the Profile Privacy Settings allowed users to 'control who can see' their profile information by selecting who could access it based on settings such as 'Only Friends' or 'Friends of Friends'. ibid 12.

However, nowhere was it informed that a user's choice to restrict access to profile information to 'only friends' or 'friends of friends' would expose the user's personal data to app developers whose apps had been installed by the user's friends.[172]

The disclosure of personal data, which was already substantial under the Facebook API released in May 2007, was broadened under the Open Graph initiative.[173] Crucially, upon authorisation of the access token, a v1 app could remain in the background without restrictions collecting and processing users' data and the data of their whole network of friends until permissions were revoked by the user, an action that users were unlikely to perform on account of the complexity and opacity of Facebook's privacy settings. Moreover, developers were able to run multiple v1 apps, and since the Graph API v1 returned users' real Facebook user IDs, app developers and their business partners were readily able to combine and mine vast volumes of personal data collected with the aid of several Facebook apps and quizzes[174] and associate that data with the real identity of users. The consequences for privacy resulting from the design of the Graph API v1 were far reaching. According to one analyst, 'if someone wasn't on Facebook at all, you could piece together a reasonable profile of them just by extrapolating data from people they were connected to outside of Facebook. Just by getting a few thousand people to give your app access to their Facebook data, developers could gather data on the millions of people in those users' networks.'[175] The Graph API v1 was available until April 2014, at which time it was replaced with the more restrictive v2 version. Nevertheless, this newer version of the Graph API disclosed up to fourteen profile items of a user via their friends.[176]

It transpires from the above that Facebook chose to benefit app developers[177] to propel Facebook's growth instead of keeping its promise not to invade its users' privacy without

---

[172] ibid 14.

[173] In particular, in addition to access to a user' personal information detailed in footnote 157, the Graph API v1 provided apps with a number of extended permissions that enabled them to access and collect the following information about that user's friends: about me, actions, activities, birthdays, checkins, history, events, games activity, groups, hometown, interests, likes, location, notes, online presence, photo and video tags, photos, questions, relationship details, relationships, religion/politics, status, subscriptions, websites, employment history and even users' private messages contained in their message inbox (via the read_mailbox API request). Jonathan Albright, 'The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle' (*Medium*, 20 March 2018) <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747>.

[174] ibid.

[175] Matt Locke, 'How Likes Went Bad – A Brief History of Attention' (*Medium*, 25 April 2018) <https://medium.com/s/a-brief-history-of-attention/how-likes-went-bad-b094ddd07d4>.

[176] Including items about me, actions.books, actions.music, actions.news, actions.video, activities, birthday, checkins, education history, events, friends, games activity, groups. hometown, interests, likes, location, notes, online presence, photo_video_tags, photos, questions, relationship details, relationships, religion/politics, status, videos, website and work history. Symeonidis and others (n 168) 6 and Table 6.

[177] In spite of being prohibited by Facebook's application developer agreement, personal data gathered by apps could be used for advertising purposes. For example, the company CubeYou offered on Facebook a number of apps to collect the personal data of Facebook's users and then contract with advertising agencies that want to target specific types of Facebook users for ad campaigns. See Michelle Castillo, 'CubeYou Cambridge-like App Collected Data on Millions from Facebook' (8 April 2018) <https://www.cnbc.com/2018/04/08/cubeyou-cambridge-like-app-collected-data-on-millions-from-facebook.html>; See also Steel and Fowler (n 160); It is extremely easy for app developers to use Facebook users' data for advertising or other purposes they deem fit. This is because applications' codes are 'hosted on the [app developer's] own servers and are out of Facebook's control. This inherently prevents Facebook from monitoring and/or controlling the application's behavior, and impedes any proactive measures to block malicious activities.' Indeed, research has found that Facebook's apps typically interact with 'fourth parties' such as ad networks, data brokers and analytics services, and that more than 75% of Facebook apps exchange data with at least six different domains, and 10% with over 20 domains. See

their consent. It is not possible to contend with any degree of credibility that Facebook users who set their privacy settings in such a way that only their friends could view their personal information were also authorising the apps installed by such friends to access and collect said information. Moreover, upon the entry into force of the 2009 privacy policy and privacy settings update, Facebook App settings by default authorised the collection and processing of users' personal data by the apps installed by their friends, and users had to manually disable all the relevant boxes under the heading 'Apps other use' to prevent this from happening.[178] Given that Facebook's '[p]rivacy default settings are such that users are totally unaware of the fact that they have to unclick the boxes in order to prevent such data processing'[179] by their friends' apps, it is safe to argue that Facebook deceptively concealed the violation of its users' privacy it had orchestrated with app developers to boost growth. Facebook ended up settling the deception charges pressed by the FTC in this connection, and under the settlement Facebook was ordered 'to take several steps to make sure it lives up to its promises in the future, including giving consumers clear and prominent notice and obtaining consumers' express consent before their information is shared beyond the privacy settings they have established.'[180] Regrettably, living up to its promises is something entirely alien to Facebook's DNA.[181]

In turn, the 'Like' button, which represents the action of 'liking' something on Facebook whilst being elsewhere on the Internet,[182] was heralded as a tool that content providers could use to increase traffic to their websites, as well as a tool for Facebook users to share information about their interests on their Facebook profile. For example, a brand could embed on its website Like buttons next to its products, and if any Facebook user clicked on the button, the action of liking that brand could be published in the user's News Feed with a link to the brand's website. According to Facebook:

'[t]he most important and powerful plugin is the Like button, which can be placed on any object (your web page, an image, an article) so that people can create connections to it and share it with their friends back on Facebook – giving you greater distribution across the web.'[183]

The installation of the Like button was simple,[184] as it only required the inclusion of a piece of HTLM Facebook code on the website free of charge.[185] Drawn by the prospect of increased traffic, and therefore more profits,[186] website publishers quickly adopted this new

---

Abdelberi Chaabane and others, 'A Closer Look at Third-Party OSN Applications: Are They Leaking Your Personal Information?', *International Conference on Passive and Active Network Measurement* (Springer 2014).

[178] Symeonidis and others (n 168) 7.

[179] ibid.

[180] FTC, 'Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises' (*Federal Trade Commission*, 29 November 2011) <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

[181] See for example text accompanying footnote 191.

[182] Facebook, 'Facebook Brand Resource Center - Assets and Brand Guidelines' (*Brand Resource Center*) <https://en.facebookbrand.com/>.

[183] Facebook, 'How to Use the New Facebook Social Plugins for Your Business' <https://www.facebook.com/notes/facebook-for-developers/how-to-use-the-new-facebook-social-plugins-for-your-business/394310302301/>.

[184] This also applies to other Social Plugins such as the Share button, the Comments box and Embedded posts.

[185] Facebook, 'Like Button for the Web' (*Facebook for Developers*) <https://developers.facebook.com/docs/plugins/like-button>.

[186] As the majority of content publishers monetise their websites through advertising, more traffic increases their profitability, as more visitors are likely to click on ads.

feature. Facebook reported that over 50,000 websites added Social Plugins within the first week of availability, including popular publishers such as Time.com, TechCrunch, NYTimes.com, WSJ.com and the Huffington Post.[187] The penetration rate of the Like button in the top 10,000 websites reached over 4% within the first six months after its launch.[188] Since the average 'liker' (that is, a user who clicks on the Like button) has 2.4x the amount of friends than that of, and clicks on 5.3x more links to external sites than the typical Facebook user, many website publishers saw increases in traffic since adding Social Plugins,[189] thereby leading to widespread adoption.[190]

The problem, again, was the Like button's design. Since it is a piece of HTML code, every time a user visits a website featuring the Like button a request for content is made to Facebook's server to provide the image when the website is loaded. Therefore, just as was the case of Beacon, Facebook could avail itself of the Like button to place and read cookies, and consequently to track users visiting websites embedded with it. Unsurprisingly, Facebook was doing exactly that, and more. In early 2011, privacy researcher Roosendaal demonstrated that not only was Facebook collecting browsing data of its users with the aid of cookies, regardless of whether they had actually clicked on the button, but also browsing data of people not having a Facebook account.[191] His findings were confirmed by an investigation conducted by the Wall Street Journal, which reported that Facebook collected people's browsing data from 331 of the most-popular 1,000 websites.[192]

Facebook quickly denied the findings. Then-Facebook's chief technology officer Bret Taylor emphatically stated: '[w]e don't use [Social Plugins] for tracking and they're not intended for tracking'.[193] He also asserted that Facebook uses cookies that are placed on the computers of people visiting Facebook's home page to protect Facebook users' accounts from cyberattacks. Moreover, that Facebook had already discontinued the collection of browsing data about people not having a Facebook account exposed by Roosendaal, which had been caused by a 'bug'.[194] To dissipate privacy concerns, retain user trust, prevent consumer switching and possibly the revival of its main competitor MySpace or the emergence of a new competitive threat, Facebook systematically continued denying the tracking accusations. For example, in September 2011 a Facebook spokesperson told CBS News:

'Facebook does not track users across the web. Instead, we use cookies on social plugins to personalize content (e.g. Show you what your friends liked), to help maintain and improve what we do (e.g. Measure click-through rate), or for safety and security (e.g. Keeping underage kids from trying to signup with a different age). No information we

[187] Facebook, 'How to Use the New Facebook Social Plugins for Your Business' (n 183).
[188] Built With, 'Facebook Like Usage Statistics' <https://trends.builtwith.com/widgets/Facebook-Like>.
[189] Facebook, 'The Value of a Liker' (29 September 2010) <https://www.facebook.com/notes/facebook-media/value-of-a-liker/150630338305797> accessed 10 April 2019.
[190] According to estimates, there are 11,377,428 websites using the Like button, including historical. Built With (n 188).
[191] Roosendaal (n 130) 5–8.
[192] Amir Efrati, "'Like" Button Follows Web Users' *Wall Street Journal* (18 May 2011) <https://www.wsj.com/articles/SB10001424052748704281504576329441432995616>.
[193] ibid.
[194] ibid.

receive when you see a social plugins is used to target ads, we delete or anonymize this information within 90 days, and we never sell your information.'[195]

Later, in December 2012, in connection with a finding of the Wall Street Journal that Facebook's Social Plugins now appeared on two-thirds of the websites surveyed, Facebook reasserted that it only used data from unclicked Like buttons for security purposes and to fix bugs in its software.[196] However, Facebook was carefully making the necessary arrangements to implement its plan of widespread surveillance for commercial purposes. In November 2012, Facebook introduced a number of changes in its privacy policy which included *inter alia* the abolition of users' ability to vote on changes to said policy,[197] the ability to use information about users and their activity on Facebook as a means for targeting ads on third party websites (at a time where it did not serve ads off Facebook), and the ability to share user information with its 'affiliates' (that is, companies owned by Facebook, such as Instagram).[198] Crucially, the privacy policy now featured a detailed section on 'Cookies, pixels and other similar technologies', explaining that Facebook uses these technologies to 'enable features and store information about you' and to 'deliver, understand and improve advertising.'[199] By way of example, Facebook noted that it could use such technologies 'to know you are logged in to Facebook, *to help you use social plugins and share buttons*, or to know when you are interacting with our advertising or Platform partners'[200] (emphasis added). A loose interpretation of these amendments could have arguably amounted to a disclosure of Facebook's imminent implementation of widespread commercial surveillance. However, this practice had not been yet explicitly informed.

That changed in June 2014. Empowered by over 1.31 billion monthly average users,[201] widespread adoption of Social Plugins across the Internet[202] and virtually no meaningful competition,[203] Facebook finally backtracked for good on its promise not to track its users'

---

[195] Eric Sherman, 'Facebook's New Privacy Bust: Users Log In but They Can't Log Out [Update]' (*CBS News*, 26 September 2011) <https://www.cbsnews.com/news/facebooks-new-privacy-bust-users-log-in-but-they-cant-log-out-update/>; Also, Facebook Help Center at the time contained the following statement: 'We do not share or sell the information we see when you visit a website with a Facebook social plugin to third parties and we do not use it to deliver ads to you. In addition, we will delete the data (i.e. data we receive when you see social plugins) associated with users in 90 days. We will keep aggregated and anonymized data (not associated with specific users) after 90 days for improving our products and services.' Emil Protalinski, 'Facebook Denies Cookie Tracking Allegations' (*ZDNet*, 25 September 2011) <https://www.zdnet.com/article/facebook-denies-cookie-tracking-allegations/>.

[196] Julia Angwin, 'It's Complicated: Facebook's History of Tracking You' (*ProPublica*, 17 June 2014) <https://www.propublica.org/article/its-complicated-facebooks-history-of-tracking-you>.

[197] See above footnote 151.

[198] Kashmir Hill, 'What You Actually Need To Know About The Changes Facebook Is Making To Its Privacy Policy' (*Forbes*, 2012) <https://www.forbes.com/sites/kashmirhill/2012/11/26/what-you-actually-need-to-know-about-the-changes-facebook-is-making-to-its-privacy-policy/#6be19f6a148d>; Mathew Ingram, 'Facebook Makes It Official — an External Advertising Network Is Coming Soon' (23 November 2012) <https://gigaom.com/2012/11/23/facebook-makes-it-official-an-external-advertising-network-is-coming-soon/>.

[199] 'Facebook Fleshes Out Privacy Policy To Comply With Data Protection Audits, Will Hold Q&A On Monday' (*TechCrunch*, November 2012) <http://social.techcrunch.com/2012/05/11/facebook-privacy-policy-changes/>.

[200] ibid.

[201] Statista, 'Facebook Users Worldwide 2018' (*Statista*) <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>.

[202] Built With (n 188).

[203] Rivals such as MySpace, BlackPlanet, Yahoo's 360, Bebo and Friendster had already exited the market.

activities on third party websites and apps for commercial purposes,[204] this time without risking consumer switching. Soon thereafter, under the highly misleading and somewhat irritating heading 'Helping you Understand How Facebook Works and How to Control your Information,'[205] Facebook announced on 13 November 2014 a new update of its terms and policies, including its privacy policy (the '2015 Data Policy'). This update, which came into force on 1 January 2015, included explicit descriptions of Facebook's user tracking for commercial purposes, to which now consumers had to agree or close their accounts.

III. Anticompetitive Conduct by Facebook

The argument is commonly made that competition law should be concerned with competition issues only,[206] and consequently violations of online privacy and deception should be addressed by the applicable data protection and consumer protection regulatory frameworks. Both the Commission and the CJEU have endorsed this stance. In *Asnef-Equifax,* the CJEU held that '[…] since […] any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection.'[207] The Commission has expressed the same position in *Google/DoubleClick*.[208] More recently in *Facebook/WhatsApp*, it held: '[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.'[209]

This stance is sound in the majority of cases. For example, a recent data breach that affected nearly 50 million Facebook accounts[210] should be assessed under and punished by data protection law only, as Facebook admittedly did not derive any competitive benefit from it. However, in data-driven markets there is a substantial overlap between competition, data protection and consumer protection law.[211] Given that the ability to access and process data, especially personal data, is of tremendous relevance for the competitive performance of data-driven undertakings, [212] large-scale data protection

---

[204] Facebook Newsroom, 'Making Ads Better and Giving People More Control Over the Ads They See' (12 June 2014) <https://newsroom.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/>.

[205] Facebook, 'Updating Our Terms and Policies: Helping You Understand How Facebook Works and How to Control Your Information' (*Facebook Newsroom*, 13 November 2014) <https://newsroom.fb.com/news/2014/11/updating-our-terms-and-policies-helping-you-understand-how-facebook-works-and-how-to-control-your-information/>.

[206] Manne and Sperry (n 62).

[207] *Case C-238/05, Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc) [2006] ECR I-11125* 63. For an interpretation of this statement, see Alec J. Brunside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' CPI Antitrust Chronicle (May 2015) 4.

[208] *Case COMP/M4731, Google/DoubleClick (2008)* para 368.

[209] *Case COMP/M.7217, Facebook/WhatsApp (2014)* (n 15) para 164.

[210] Olivia Solon, 'Facebook Faces $1.6bn Fine and Formal Investigation over Massive Data Breach' *The Guardian* (3 October 2018) <https://www.theguardian.com/technology/2018/oct/03/facebook-data-breach-latest-fine-investigation>.

[211] EDPS, 'Preliminary Opinion of the European Data Protection Supervisor. Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' </data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en>.

[212] Indeed, §18(3a) of the German Competition Act considers access to personal data as a criterion for market power.

violations and related enabling deception that confer upon the infringer a competitive advantage are bound to impinge upon the competitive process, and therefore are cognisable by competition law. As observed by the *Autorite de la Concurrence* and the *Bundeskartellamt*: 'reductions in privacy could also be a matter of abuse control, if an incumbent collects data by clearly breaching data protection law and if there is a strong interplay between the data collection and the undertaking's market position.'[213] Alec J. Burnside neatly sums it up: '[a]ntitrust is not somehow set aside by the fact that a Big Dataset comprises information about individuals that may also be subject to privacy or data protection requirements.'[214]

As seen in Section II, Facebook has systematically deceived and violated the privacy of its users to reach scale, enhance the attractiveness of its platform, boost user engagement, drive more traffic and collect more data. As a result,it attained and entrenched a dominant position in the social network market and leveraged that position onto the display advertising market. Facebook entered the social network market picturing itself as a safe, trustworthy and privacy-centred alternative to then-market leader MySpace, quickly attracting social network users who were dissatisfied with MySpace's lax privacy controls and bad reputation.[215] However, shortly thereafter Facebook changed this approach, as data mining proved successful to propel growth. Constrained by the privacy expectations and preferences of its users, Facebook decided to engage in deception to track their behaviour off Facebook and collect more data about them with the aid of its advertising product Beacon. However, the discovery of its deception, the ensuing consumer backlash and competitive pressure forced Facebook to cancel such product and apologise for its deceiving conduct and privacy violations.[216] Yet, Facebook had already set its vision of unrestricted online surveillance of consumers for financial gains. To realise its vision, it opened its platform to app developers and gave them broad access to its users' and their friends' personal data, carefully concealing this access under deceiving and misleading privacy settings.[217] Thence, strong indirect network effects[218] propelled user growth and traffic, and consequently Facebook gained access to more data to improve its services. In particular, drawn by Facebook's already large user base and the prospect of accessing large volumes of personal data to better determine and understand Facebook users' preferences, the number of apps grew exponentially.[219] Since a higher number of apps made the platform more attractive to the user side, Facebook's user base grew even larger. Strong direct network effects[220] in turn reinforced the growth of Facebook's user base, which went from 58 million users in 2007, the year of introduction of Facebook Platform, to 608 million users in 2010,[221] the year of introduction of the Open Graph and Social Plugins, products which cemented Facebook's dominance in the social network market and paved the way for the implementation of widespread commercial surveillance. Specifically, the Open Graph reinforced the incentives for app developers to build Facebook apps, thereby fuelling indirect network effects on the user side. In turn, Facebook leveraged its growing user base to induce website publishers and apps to adopt its Social Plugins and make them

[213] Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data' (2016) 25.
[214] Alec J. Brunside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' CPI Antitrust Chronicle (May 2015) 3.
[215] See text accompanying footnotes 109, 110 and 111.
[216] See text accompanying footnote 150.
[217] See text accompanying footnote 172.
[218] See Section I.C.1.
[219] See text accompanying footnote 188.
[220] See Section I.C.1.
[221] Sedghi (n 128).

dependent on Facebook's technology to drive traffic,[222] thereby building the infrastructure to track people throughout the Internet, unbeknownst to them and contrary to Facebook's representations.[223] Finally, unrestrained by competitive pressure, Facebook fully departed from its long-standing promise not to track people online for financial gain,[224] thereby leveraging its user base and surveillance infrastructure to strengthen its position in the display advertising market.

In the course and after the culmination of this unlawful and reproachable strategy, Facebook has abused its dominant position in two main ways. Firstly, it has exploited consumers by imposing unfair trading conditions upon them (A). Secondly, it has resorted to data protection violations and deception to strengthen its dominance in the social network market, raise barriers to entry and leverage its dominant position onto the display advertising market (B).

And there is more. Facebook became an important source of traffic referrals for news publishers, in exchange for free content publishers posted on Facebook. Yet, at certain point Facebook decided to prioritise content that propelled more consumer engagement, to the detriment of publishers which saw a dramatic reduction in traffic (C). Also, the data trove that Facebook has been able to amass has given it the ability to squash potential competitive threats. In particular, Facebook has refused a number of apps access to an indispensable permission of its Graph API, thereby protecting and reinforcing its dominant position and chilling innovation incentives (D). Lastly, Facebook has resorted to deception to collect mobile usage data, and based on mobile usage trends derived from that data, it has acquired and attempted to acquire actual and potential competitors to protect its dominant position, copying its competitors' innovations when the acquisition route failed (E).

A. Exploitative Abuse: Unfair Trading Conditions

When the social network market remained to a greater or lesser extent competitive, Facebook was unable to force its users to consent to pervasive tracking across the Web for commercial purposes. Consumers fiercely resisted and shamed Beacon,[225] as well as the 2009 privacy policy and privacy settings update.[226] However, after becoming the absolute market leader and acquiring what could have been its closest competitor (Instagram), Facebook was finally free to openly backtrack on its promise not to track people off Facebook, contrary to their privacy preferences, in order to access the browsing data it needed to strengthen its position in the display advertising market and exclude competition in that sector. Put in other words, Facebook imposed on consumers contractual terms that it could not have otherwise imposed under competitive conditions, with an aim to increase its market power.

In order to determine the extent of Facebook's ability to collect and process personal data under the 2015 Data Policy, such contractual terms are analysed below (1). This analysis is necessary to illustrate that these terms are unfair within the meaning of Article 102(a)

[222] Relatedly, see Section III.C.
[223] See text accompanying footnotes 193, 194 and 195.
[224] See text accompanying footnote 204.
[225] See text accompanying footnote 144.
[226] See text accompanying footnote 163.

TFEU (2).[227] Crucially, these terms violate EU data protection law (3). This finding lends support to the argument that Facebook degraded the quality of its social networking service to reinforce its position in the display advertising market, thereby leveraging its dominant position through the exploitation of consumers (4).

1. Analysis of the Unfair Trading Conditions in the 2015 Data Policy

To sign up with Facebook, users must previously agree to its Terms of Service, Data Policy and Cookie Policy (the 'Governing Documents'). By clicking on the button 'Sign Up' on Facebook's homepage,[228] users consent to **all** of Facebook's data processing practices enabled by these documents.[229] Similarly, when there is a policy update, users are required to either agree to the entirety of them or close their accounts.

In the introduction of the 2015 Data Policy, Facebook gave the following warning:

'As you review our policy, keep in mind that it applies to all Facebook brands, products and services that do not have a separate privacy policy or that link to this policy, which we call the "Facebook Services" or "Services"'.[230]

Then, under the section 'What kinds of information do we collect?' Facebook stated:

'**Information from websites and apps that use our Services**
We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

Information from third-party partners
We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

Facebook companies
We receive information about you from companies that are owned or operated by Facebook, in accordance with their terms and policies.'[231]

---

[227] In addition, this analysis is instrumental to demonstrate that, by imposing these terms and consequently exploiting consumers, Facebook leveraged its dominant position in the social network market and the dependence of website publishers and apps on Facebook's technology to reinforce its position in display advertising, thereby foreclosing competition. See below Section III.B.
[228] 'Facebook - Log In or Sign Up' (*Facebook*) <https://www.facebook.com/>.
[229] It is a known fact that the overwhelming majority of Internet users do not engage with terms of service and privacy policies, so they tend to just 'click the box' and proceed to use the service. However, informed consumers with the intention to sign up with Facebook would have to go through all of Facebook's governing documents, including hyperlinks and terms of service and privacy policies of its affiliate companies, which is an extremely time-consuming and labour-intensive task.
[230] Facebook, 'Facebook 2015 Data Policy' (1 January 2015) <https://web.archive.org/web/20150602223258/https://www.facebook.com/privacy/explanation>.
[231] ibid.

Facebook owned the following companies at the time the 2015 Data Policy entered into force: Facebook Payments Inc., Atlas, Instagram LLC, Mobile Technologies Inc., Onavo, Parse, Moves, Oculus, LiveRail and WhatsApp Inc.[232]

Then, under the section 'How do we use this information?' Facebook informed the following:

'**Show and measure ads and services.**
We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services.'[233]

Lastly, under the heading 'How is this information shared?' Facebook informed:

'Sharing within Facebook companies.
We share information we have about you within the family of companies that are part of Facebook.'[234]

It follows from the above that Facebook aggressively expanded the data collection points across the web, as well as the entities with which the data Facebook held about its users could be shared. Now, it could collect users' personal data from third party websites and apps that used any of the 'Facebook Services' (which not only now included websites and apps embedded with Social Plugins, but also websites and apps using Facebook's advertising and analytics services), from 'third-party partners' (whatever that was), from advertisers and from all of the 'Facebook companies', including the popular Instagram. It could also share back all of this information with its own companies. Crucially, this information could be combined with the personal data users provided on Facebook to create exhaustive user profiles, as the additional data collected off Facebook revealed what users did elsewhere on the web,[235] as a result of which their preferences, interests and even intimate details could be inferred or identified with remarkable precision. These profiles, in turn, could be used to serve ads on and off Facebook (through its 'Facebook Audience Network' initiative[236]), thereby extending Facebook's 'data profiling and ad-targeting juggernaut from its own apps and services to the rest of the internet.'[237]

There was not much users could do with regard to these new data processing practices. The pictures, videos, experiences and other content they shared on the platform, and the friend connections they made throughout the years, effectively locked them in.[238] This was especially the case of those users that joined Facebook from its inception, at a time where it presented itself as a privacy-driven social network. In turn, people who wanted to join but did not approve of Facebook's extensive surveillance did not have viable alternatives in the market. Facebook offered an opt-out mechanism for those who did not want to be tracked on external websites and apps for what it called 'interest-based advertising',

[232] Facebook, 'The Facebook Companies' (*Facebook Newsroom*, 2015) <https://web.archive.org/web/20150530121902/https://www.facebook.com/help/111814505650678>.
[233] Facebook, 'Facebook 2015 Data Policy' (n 230).
[234] ibid.
[235] See text accompanying footnotes 130 and 131.
[236] Facebook, 'Introducing Facebook Audience Network' (*Facebook for Business*, 30 April 2014) <https://www.facebook.com/business/news/audience-network>.
[237] Albright (n 173).
[238] For a solution to this switching cost, see Sections IV.B.1 and IV.B.2.

providing a link to the European Interactive Digital Advertising Alliance.[239] However, research demonstrated that the opt-out process was ineffective. Acar *et al* found that 'even if a Facebook users [sic] opts-out from interest-based advertising and logs out from her account, Facebook still tracks her browsing activity through social plug-ins[, and] one of the cookies collected by Facebook is, according to Facebook's 2012 statements, used for advertising purposes.'[240] Moreover, there were no options to opt-out from data collection from the 'Facebook Companies', let alone from the combination of that data with other data collected on and off Facebook for advertising on Facebook.

Ultimately, on 1 January 2015, consumers were confronted with a binary choice: either accepting the entirety of Facebook surveillance apparatus, or not using Facebook at all. Facebook's surveillance has worsened ever since, given that its latest Data Policy[241] retains the same terms above (albeit explained in a somewhat more detailed manner) and the amount of Facebook Services to which said policy applies (now branded Facebook Products) has increased significantly.[242]

2. Unfairness within the Meaning of Article 102(a) TFEU

The terms of Facebook's 2015 Data Policy and its last version that allow Facebook to track its users off Facebook across millions of websites and apps, and to combine their browsing data with data collected on Facebook and other services it owns, to which users are forced to agree as a precondition to use Facebook, are unfair within the meaning of Article 102(a) TFEU.

The term 'unfair' is not defined in Article 102 TFEU. Its meaning, however, can be deduced from the case law of the EU Courts and the Commission's decisional practice.

In *BRT v SABAM*, certain questions on the interpretation of Article 86 EEC [now 102 TFEU] were filed with the CJEU, *inter alia,* whether an undertaking which enjoys a *de facto* monopoly in a Member State for the management of copyrights abuses its dominant position by demanding the global assignment of all copyrights without drawing any distinction between specific categories of such rights.[243] The CJEU held that, to appraise whether there is abuse in this sense, all *relevant interests must be taken into account in order to ensure balance* between the requirement of maximum freedom for the members of the

---

[239] Facebook, 'About Advertising on Facebook' (2015) <https://web.archive.org/web/20150530121908/https://www.facebook.com/about/ads/#568137493302217>.

[240] Güneş Acar and others, 'Facebook Tracking through Social Plug-Ins' (2015) Technical Report prepared for the Belgian Privacy Commission.

[241] Facebook, '2018 Data Policy' (*Facebook*) <https://www.facebook.com/about/privacy/update/draft2?CMS_BRANCH_ID=1534594943262990>.

[242] According to Facebook: 'The Facebook Products include Facebook (including the Facebook mobile app and in-app browser), Messenger, Instagram (including apps like Direct and Boomerang), Portal-branded devices, Moments, Bonfire, Facebook Mentions, Spark AR Studio, Audience Network, and any other features, apps, technologies, software, products, or services offered by Facebook Inc. or Facebook Ireland Limited under our Data Policy. The Facebook Products also include Facebook Business Tools, which are tools used by website owners and publishers, app developers, business partners (including advertisers) and their customers to support business services and exchange information with Facebook, such as social plugins (like the "Like" or "Share" button) and our SDKs and APIs.' Facebook, 'What Are the Facebook Products? | Facebook Help Centre' <https://www.facebook.com/help/1561485474074139?ref=dp>.

[243] *Case 127/73, Belgische Radio en Televisie v SV SABAM and NV Fonior (SABAM) [1974] ECR 313*.

undertaking and the effective management of their rights by the latter.[244] The CJEU concluded that a dominant undertaking abuses its position when it 'imposes on its members obligations which are *not absolutely necessary* for the attainment of its object and which thus *encroach unfairly upon a member's freedom* to exercise his copyright.[245]

Similarly, in GEMA, an amendment to a dominant undertaking's statutes was challenged as unfair within the meaning of Article 102(a) TFEU, as they limited the undertaking's members' freedom to exploit musical works. Basing its decision on *BRT v SABAM*, the Commission held that to determine whether the undertaking's statutes constitute an abuse 'the decisive factor is whether they exceed the limits absolutely necessary for effective protection (indispensability test) and whether they limit the individual copyright holder's freedom to dispose of his work no more than need be (equity).'[246] These two cases suggest some sort of proportionality test to determine when terms and conditions are unfair, and therefore abusive.

Moreover, in *DSD*, the Commission found a breach of Article 102(a) as '[u]nfair commercial terms exist where an undertaking in a dominant position fails to comply with the principle of proportionality.'[247] When asserting the foregoing, the Commission referred to paragraph 190 of *United Brands*, where the CJEU held that the possibility of a counter-attack by a dominant undertaking must be 'proportionate' to the threat, taking into account the economic strength of the undertakings confronting each other. Accordingly, the 'fairness' or 'unfairness' of the relevant commercial terms seems to be dependent on the economic strength of the dominant undertaking relative to its customers or consumers.

In a similar vein, in *AAMS,* the dominant undertaking, which was part of the Italian financial administration involved in the exclusive production, export and wholesale distribution of tobacco, was found to have abused its dominant position by including unfair clauses in its distribution contracts. These clauses *inter alia* limited foreign firms' ability to increase the number of cigarettes put on the market and imposed cumbersome inspection obligations in respect of imported cigarettes. Broadly, the Commission found that the terms were not necessary in view of the object of the contract. On appeal the General Court found that 'the inspections [were] disproportionate and needless.'[248]

It transpires from the above that terms and conditions are unfair within the meaning of Article 102(a) TFEU when they are (i) not necessary for the achievement of the contract's object, which must balance the interest of the relevant parties, and (ii) disproportionate, taking into consideration the economic strength of the dominant undertaking relative to its customers or consumers.

(i) Necessity

The concept of necessity has its own independent meaning in EU Law.[249] The 'necessity' test asks: 'is the measure concerned necessary (indispensable) to realising the goals it is

[244] ibid para 10. Emphasis added.
[245] ibid para 15. Emphasis added.
[246] *Case IV/29971, GEMA statutes (1981)* para 36.
[247] *Case COMP D3/34493, DSD (2001)* para 112.
[248] *Amministrazione Autonoma dei Monopoli di Stato (AAMS) v EC Commission* [2001] General Court T-139/98, ECR II-3413 para 83.
[249] *Case C-524/06, Heinz Huber v Bundesrepublik Deutschland [2008] ECLI:EU:C:2008:724* para 52.

aimed at meeting?'[250] In the case at hand, the natural question to ask is: are the terms assessed in Section III.A.1 necessary for realising the object of the contract into which Facebook enters with its users?

Facebook's Governing Documents constitute the contract containing the terms the necessity of which must be determined. As a preliminary matter, the object of that contract has to be established. Facebook is a multisided, data-driven, advertisement-based business. Facebook provides to its users, free of monetary charge, a confined virtual place where they can connect with each other and share and enjoy content in different forms. In turn, for a price, Facebook allows advertisers to catch the attention of its users and serve them ads that are as targeted as possible to their revealed interests and preferences. To this effect, it collects and processes its users' personal data both to provide the social networking experience on the user side (for instance, to display social interactions that are relevant to the user) and to provide targeted advertising services on the advertiser side.[251] The provision of these two services to two separate groups of customers, therefore, is the object of Facebook's Governing Documents.

This object must balance the interests of the parties. Facebook's interest is to collect and process as much data as possible to improve its social network algorithms to drive more engagement, traffic and user growth, and perhaps more importantly, to improve its ad targeting capabilities to earn more profits. In turn, users' interest is to enjoy a social networking experience based on a reasonable expectation of privacy consistent with the free character of Facebook's social network.[252] Accordingly, the interests of the parties are balanced when Facebook collects and processes personal data generated through the use of Facebook for advertising purposes, as they pay no monetary price.[253]

Having been clarified the Governing Documents' balanced object, it is now possible to determine whether the terms in question are necessary to its attainment. For terms to be 'necessary', they must be indispensable, that is to say, there must be no equally effective alternatives to achieve the contract's balanced goal with less exploitative effects.[254] It follows that contractual terms that are useful for or facilitate the performance of a contract, or which render such performance more profitable for one of the parties, are not necessary.

The terms analysed in Section III.A.1 caused exploitative effects by tilting the balance between the interests of the parties in favour of Facebook, as the data collection they enabled takes place off Facebook in a manner contrary to its users' reasonable expectation of privacy. Since the contract's balanced goal had been achieved prior to their inclusion in Facebook's Governing Documents,[255] the terms in question can hardly be indispensable.

---

[250] Lee A Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power', *in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds), Reinventing Data Protection?* (Springer 2009) <http://link.springer.com/content/pdf/10.1007/978-1-4020-9498-9_9.pdf>.

[251] See generally Section I on Facebook's business model.

[252] Lilian Edwards and Ian Brown, 'Data Control and Social Networking: Irreconcilable Ideas?', *In Andrea M. Matwyshyn (ed), Harboring Data: Information Security, Law, and the Corporation* (Standford University Press 2009).

[253] As the Bundeskartellamt observes, '[u]sers have to expect a certain processing of their data if they use' Facebook's free service. Bundeskartellamt (n 88) 2.

[254] Robert O'Donoghue and Atilano Jorge Padilla, *The Law and Economics of Article 82 EC* (Hart Publishing 2006) 654.

[255] Facebook had been earning healthy profits up until Q4 2004. Indeed, Facebook's annual net income rose from USD 53 million in 2012 to USD 2,940 million in 2014. See Forms 10-K "Annual Report

Moreover, by aggressively expanding the scope of data collection, such terms only make the achievement of the Governing Documents' object more profitable. Indeed, Facebook's chief financial officer, Dave Wehner, has acknowledged that improvements of data privacy have a negative impact on Facebook's revenue growth.[256] Therefore, the terms in question fail to meet the necessity criterion, and therefore are unfair within the meaning of Article 102(a) TFEU. Nevertheless, for the sake of completeness, the question of whether such terms meet the proportionality requirement is addressed below.

(ii) Proportionality

As O'Donoghue and Padilla observe, proportionality requires a balancing between the object of the contract, the terms subject to scrutiny, and the contractor's justification for those terms.[257] Accordingly, the terms in question should (a) have a legitimate objective, (b) be capable of achieving that objective, (c) be necessary, in the sense explained in paragraph (i) above, and (d) be proportionate, meaning that the legitimate object of the terms must outweigh the exploitative effects on the other party to the contract,[258] taking into account the position of strength of the parties involved.

It was seen above that the terms in question significantly increased Facebook's data collection scope to improve its ad targeting algorithms, and therefore Facebook was seeking to increase its profitability. This objective is a legitimate one, and said terms are certainly capable of achieving it. Given that necessity was analysed in paragraph (i) above, the last issue to consider is whether the negative effects of the terms outweigh the positive gains of their legitimate object.

The terms in question benefited both Facebook, and in the short-run, advertisers, as improvements in ad targeting are positively correlated with their ROI. However, in the medium to long-run, these terms will have negative effects for advertisers, since Facebook is increasingly becoming an unavoidable trading partner for them, a fact that is reflected by the rapidly growing turnover Facebook has generated since the year of implementation of the terms in question.[259] Advertisers have already begun to complain about a number of practices by Facebook that reflect its market power in the display advertising market.[260] Therefore, there is 'potential for competitive harm on the side of the advertising customers who are faced with a dominant supplier of advertising space.'[261]

On the other hand, the terms under analysis had extremely negative effects on Facebook users, as they almost entirely eliminated their scope of choice as to whether they accepted

---

pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934" for the fiscal years ending on 31 December 2012 to 31 December 2014, filed by Facebook with the U.S. Securities and Exchange Commission, available at https://www.sec.gov/cgi-bin/browse-edgar?company=facebook&owner=exclude&action=getcompany

[256] Facebook, 'Facebook Inc. Q2 2018 Earnings Conference Call' <https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Earnings-call-prepared-remarks.pdf>.

[257] O'Donoghue and Padilla (n 255) 654.

[258] ibid 654–655.

[259] Facebook's annual advertising revenues rose from USD 17,079 million in 2015 to USD 55,013 million in 2018. See Forms 10-K "Annual Report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934" for the fiscal years ending on 31 December 2015 to 31 December 2018, filed by Facebook with the U.S. Securities and Exchange Commission, available at https://www.sec.gov/cgi-bin/browse-edgar?company=facebook&owner=exclude&action=getcompany

[260] See text accompanying footnotes 384 to 390.

[261] Bundeskartellamt (n 88) 4.

being permanently and relentlessly tracked online. Upon the entry into force of the terms in question, Facebook users had to choose either to accept being tracked online or to close their Facebook accounts, and even this last choice would not prevent that tracking: Facebook places cookies on the browsers of people visiting websites and apps embedded with Facebook's Social Plugins or using Facebook's advertising and/or analytics services regardless of whether they have a Facebook account,[262] and as research has proved,[263] Facebook's opt-out mechanism for behavioural ads off Facebook does not prevent Facebook from placing cookies and tracking. Moreover, consumers that were dissatisfied with the imposition of the terms and wanted to switch to competing social networks had nowhere to go, since Facebook controls the second largest social network, Instagram, which is subject to the same terms that enable tracking and combination of data. This fact reflects Facebook's overwhelming strength and bargaining power relative to its users. Indeed, it is Facebook's dominance the factor that enables it to impose onerous terms, which could not be imposed under competitive conditions.

In addition, the negative effects on Facebook users are worsened by the extent of the privacy intrusions arising from Facebook's data processing activities enabled by the terms in question. By being able to track people throughout the Web and combine their browsing data with data collected on Facebook and its other services to create detailed user profiles, Facebook is excessively encroaching upon its users' data privacy, not least because Facebook ties the Facebook IDs of its users with tracking cookies. So if a user is visiting a website embedded with Social Plugins to seek information on, for example, a complicated illness or drug addiction recovery, instead of relating that information to the user's Cookie ID, Facebook could link it to the user's actual identity.[264] Importantly, if the user deletes Facebook's cookies from its browser, that information would nevertheless remain in its user profile compiled by Facebook under his real identity.[265] As the Article 29 Working Party observes '[a]ssessing impact [on data subjects' data privacy] may involve considering […] whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling […]) Seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data [...] Depending on the nature and impact of these predictions, this may be highly intrusive to the individual's privacy.'

Given that terms in question only benefit Facebook and advertisers in the short-run, but will cause significant negative effects in medium- to long-run in the display advertising market by reinforcing Facebook's already strong position in that segment, eliminated consumer choice in the social network market and enabled excessive intrusions into consumers' private life, such terms fail to meet the proportionality requirement.

3. Violations of EU Data Protection

[262] Under the heading 'Where do we use cookies?' of Facebook Cookie Policy, Facebook explains that it places cookies on people's computers or devices when they use or visit '[w]ebsites and apps provided by other companies that use the Facebook Products, including companies that incorporate the Facebook Technologies into their websites and apps [...] This occurs whether or not you have a Facebook account or are logged in." Facebook, 'Cookie Policy' <https://www.facebook.com/policies/cookies/>.
[263] See text accompanying footnote 240.
[264] For example, instead of 'user 876876876 was reading the article "What to do when you have a drug addiction" on www.theguardian.co.uk', Facebook can determine 'Tomas Llanos was reading the article "What to do when you have a drug addiction" on www.theguardian.co.uk.'
[265] Srinivasan (n 138) 74–75.

It was seen in Section II that Facebook has a long-standing record of deceptive practices and privacy violations aimed at driving more traffic, growth, disclosure of personal data, profits and ultimately achieving a dominant position in the social network market.[266] The imposition of the exploitative terms assessed above, and generally the manner in which Facebook elicits user consent to its data processing operations, are more manifestations of Facebook's privacy-intrusive modus operandi to reinforce its market position at the expense of consumers' data privacy rights. Congruently, stronger and fierce enforcement of the data protection law is required to restore competition in the social network market.[267]

Moreover, the fact that the exploitative terms violate EU data protection law supports the view that Facebook degraded the quality of its social network service to reinforce its position in the display advertising market, for which reason the exploitation of consumers is directly linked to the exclusion of competition in the latter segment.

The manner in which the exploitative terms introduced in the 2015 Data Policy violate EU data protection law is presented below. Since those terms remain in Facebook's most recent (2018) Data Policy, the analysis focuses on this document.

The collection and processing of personal data requires a legal basis.[268] Facebook may in principle invoke the following bases to legitimise its data processing operations:

- necessity for the performance of the contract: this basis applies only to processing that is strictly necessary to provide the social networking services (for example, initial creation of profiles, offering of basic functionalities);[269]
- (overriding) legitimate interests pursued by the controller: this basis applies only to a very limited number of operations, such as processing in order to ensure system security;

[266] Commenting on the Cambridge Analytica scandal, former FTC Commissioner David Vladeck, who worked in the investigation that led to the 2011 consent decree, commented: 'All of this leads back to the question whether Facebook is a venal company that warrants especially harsh treatment from regulators. Facebook now has three strikes against it: Beacon, the privacy modifications it made in 2009 to force private user information public, and now the Kogan/Cambridge Analytica revelation. Facebook can't claim to be clueless about how this happened. The FTC consent decree put Facebook on notice. All of Facebook's actions were calculated and deliberate, integral to the company's business model, and at odds with the company's claims about privacy and its corporate values. So many of the signs of venality are present.' David Vladeck, 'Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal? (Harvard Law Review) |' (4 April 2018) <https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/>.

[267] See Section IV.A.1.

[268] See Article 6 GDPR.

[269] According to the Article 29 Working Party, this legal basis 'must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some data processing is covered by a contract does not automatically mean that the processing is necessary for its performance. For example, Article 7(b) [of Directive 95/46/EC] is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them "necessary" for the performance of the contract.' Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217' (2014) 16.

- for all other processing operations, including the processing of users' personal data for profiling, tracking[270] and ad targeting, Facebook must obtain the consent of its users.

For consent to be valid, it must be 'freely given' (a), 'specific' (b), 'informed' (c) and 'unambiguous' (d).[271] Since Facebook requires to join and use Facebook that users consent to **all** of its data processing operations, including the tracking off Facebook and combination of their browsing data with data gleaned from Facebook and from any of its plethora of products and services, as described in its 2018 Data Policy,[272] the analysis of the consent that Facebook elicits from its users must consider all of its data processing operations as a whole.

a. Freely given

Data subjects must have the ability to exercise 'real choice' when agreeing to the processing of their personal data. Accordingly, consent will not be valid if the data subject has no genuine or real choice, feels compelled to consent or will endure negative consequences if he/she does not consent to the terms of service and/or privacy policy offered.[273]

In practice, there are a number of factors that undermine a user's ability to 'freely' provide consent to Facebook's data processing operations.

Firstly, as indicated in Recital 43 of the GDPR, '[…] consent should not provide a legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller […] and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.' Although this Recital is specifically concerned with public authorities, 'imbalances of power are not limited to public authorities and employers',[274] and they may arise in situations where controllers are private entities such as Facebook. Specifically, an imbalance of power between Facebook and its users arises from the dominant position Facebook holds in the market for social networking services. One of the primary reasons for joining is the fact that 'everyone is on it'. So there are no credible competitors. In addition, oftentimes having a Facebook account is a requirement for using other popular applications such as, for example, Tinder. The second largest social network, Instagram, is also controlled by Facebook, so a user must either accept Facebook's 2018 Data Policy (which applies to data processing operations on Instagram) or not be on social networks altogether. Moreover, since Facebook is a closed proprietary network and therefore messages, updates, events and other content are shared and can be accessed only on Facebook, there is a kind of social pressure to continue using it. Direct network effects and lock-in effects compound

[270] Indeed, under Article 5(3) of the E-Privacy Directive a social network provider must obtain the consent of its users prior to (i) the installation of any software on the device of an end-user (e.g., when offering a mobile application for the social network); and (ii) any placement of cookies which are not strictly necessary to provide the service (e.g., to monitor web-browsing activities outside the social network). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 s 5(3).
[271] 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 (General Data Protection Regulation) OJ L119/1 s 4(11).
[272] Facebook, '2018 Data Policy' (n 241).
[273] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018).
[274] ibid 7.

this pressure. For example, longstanding users normally have invested substantial time and effort to build a profile and a network of friends on Facebook. If a longstanding user had decided, for instance, not to agree to Facebook's last update of Governing Documents,[275] he would have lost access to valuable personal information and connections that could be important for his personal, social and even professional life.

Secondly, an individual's ability to withhold consent is constrained by Facebook's conditional terms to use the service. According to Article 7(4) of the GDPR, to assess whether consent if freely given 'utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.' This is confirmed by Recital 43 of the GDPR, according to which '[c]onsent is presumed not to be freely given (…) if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.' Since Facebook conditions access to its social network on the processing of its users' personal data for many purposes that are not necessary for the provision of the social network service, such as for example, to show ads off Facebook or to improve some of its products such as Instagram or WhatsApp, users are not in a position to exercise genuine choice. This is inconsistent with the spirit of the GDPR, which seeks to ensure 'that the processing of personal data for which consent is sought [does not] become directly or indirectly the counter-performance of a contract.'[276]

Thirdly, Facebook's 'all-or-nothing' approach prevents its users from exercising genuine choice as to certain data processing operations. Facebook requires that users consent to its Governing Documents as a whole, and therefore relies on an overall bundled consent to carry out any of the operations described therein. It is not possible, for example, to consent only to the basic social network features while not consenting to the use of personal data gathered off Facebook for commercial profiling. According to the Article 29 Working Party, '[c]onsidering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioural advertising in order to avoid the risk of being partially excluded from social interactions. The user should be put in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service. A pop-up box could be used to offer the user such a possibility.'[277] This position is supported by Recital 43 of the GDPR, which provides that consent 'is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.'

Fourthly, consent cannot be regarded as freely given if the data subject is unable to refuse or withdraw consent without detriment.[278] For example, downgrading a service would amount to a situation where there is detriment to the data subject should he decide to

[275] Facebook, 'We're Making Our Terms and Data Policy Clearer, Without New Rights to Use Your Data on Facebook | Facebook Newsroom' (4 April 2018) <https://newsroom.fb.com/news/2018/04/terms-and-data-policy/>.
[276] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 274) 8.
[277] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of "Consent"' (2011) 18.
[278] 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 (General Data Protection Regulation) OJ L119/1 Recital 42.

withdraw consent.[279] However, Facebook goes beyond downgrading the social network service should a user choose to withdraw consent, as in this case Facebook ceases to provide the social network service altogether. Indeed, when Facebook updates its Governing Documents, existing users have only two options: either to consent to the new terms or delete their Facebook account.

In view of the above, the consent Facebook obtains from its users is forced, as opposed to freely given.

b. Specific

To be valid, consent must clearly and precisely refer to the scope and consequences of the relevant data processing operation. It cannot apply to an open-ended set of processing activities. Consent 'notably includes which data are processed and for which purposes.'[280] Put in other words, 'specific' means that the data subject's expression of will must relate to a specific data processing operation or a well-defined category of data processing.[281] Facebook's 2018 Data Policy clearly lacks such specificity, especially with regard to how it uses this data.

For example, the 2018 Data Policy informs:

'We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things such as helping you and others find people you may know […]

To create personalised Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data that we collect and learn from you and others […]'[282]

In addition, it is unclear the precise extent to which users' data is collected from and shared with other entities such as the 'Facebook Companies' and 'Partners' (which include advertisers, app developers and publishers), as well as what is the exact identity of these entities. The Article 29 Working Party has already stressed this issue with regards to apps in social networks:

'Considering that the application can run without it being necessary that any data is transferred to the developer of the application, the WP encourages granularity while obtaining the consent of the user, i.e. obtaining separate consent from the user for the transmission of his data to the developer for these various purposes. Different mechanisms, such as pop-up boxes, could be used to offer the user the possibility to select

[279] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 274) 11.
[280] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of "Consent"' (n 278) 17.
[281] As explained by the Article 29 Working Party: "[B]lanket consent without specifying the exact purpose of the processing is not acceptable… [Consent] should refer clearly and precisely to the scope and consequences of the data processing. It cannot apply to an open-ended set of processing activities… Consent must be given in relation to the different aspects of the processing, clearly identified. It includes notably which data are processed and for which purposes." ibid.
[282] Facebook, '2018 Data Policy' (n 241).

the use of data to which he agrees (transfer to the developer; added value services; behavioural advertising; transfer to third parties; etc.).'[283]

c. Informed

'Informed' means that the user's consent ought to be based on an appreciation and understanding of the facts and implications of an action. The individual concerned 'must be given, in a clear and understandable manner, accurate and full information of all relevant issues […] such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject. This includes also an awareness of the consequences of not consenting to the processing in question.'[284] Accordingly, all information necessary for the data processing operation must be provided at the time the consent is requested, addressing all of the substantial aspects of the processing in respect of which the consent is needed.[285] For example, subjects of location data must be previously informed about the identity of the controller, the purposes of processing, the type of location data processed, the duration of processing, whether the data will be transmitted to a third party, the right of access to and the right to rectify the data, the right to withdraw consent or temporarily refuse the processing of such data, and the right to cancel the data.[286]

Two significant considerations apply to this requirement: Firstly, the way the information is given (in plain text, without use of jargon, understandable, conspicuous) is crucial in assessing whether the consent is 'informed'. The way in which this information should be given depends on the context: a regular/average user should be able to understand it. Secondly, information must be given directly to individuals. It is not enough for information to be 'available' somewhere. The information must be clearly visible (type and size of fonts), prominent and comprehensive.[287]

Facebook fails to define in precise terms the purposes for which user data will be processed. The same applies with regard to its description of the (categories of) recipients of the data. This situation is compounded by the fact that the 2018 Data Policy contains several hyperlinks to 'learn more' about certain data processing operations (such as how Facebook selects and personalises ads) or about how information is received from and shared with third parties. In addition, the 2018 Data Policy must be read in conjunction with the Cookie Policy in order to be able to grasp better Facebook's plethora of complex data practices, especially with regard to the tracking enabled by Facebook's exploitative terms. This method to provide information to users fails to meet the 'informed' requirement.

d. Unambiguous

Unambiguous means that the action by the user can only be understood as an expression of his agreement that personal data relating to him will be processed.

---

[283] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of "Consent"' (n 278) 19.
[284] Article 29 Data Protection Working Party, 'WP131 - Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records.' (2007) 9.
[285] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of "Consent"' (n 278) 9.
[286] Article 29 Data Protection Working Party, 'Opinion on the Use of Location Data with a View to Providing Value-Added Services 2130/05/EN WP 115' (2005) 4–5.
[287] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of "Consent"' (n 278) 20.

Default settings which are configured to disclose information without the active engagement of the user do not produce unambiguous consent. When certain settings which are not crucial to use the social network service 'overshare' data by default (for example, with friends-of-friends or app developers), users are required to take active steps to undo this. According to Article 29 Data Protection Working Party, it is questionable, 'whether not clicking on the button means that individuals at large are consenting.'[288]

The 2018 Data Policy informs:

'We use the information we have about you – including information about your interests, actions and connections – to select and personalise ads, offers and other sponsored content that we show you. Learn more about how we select and personalise ads, and your choices over the data we use to select ads and other sponsored content for you in the Facebook Settings and Instagram Settings.'[289]

It is highly debatable whether the manner in which users' choices about the data Facebook uses for advertising complies with the requirement of 'unambiguous' consent. On Facebook's Ad settings interface, users must disable a number of options to prevent certain types of advertising, such as the options to stop seeing ads off Facebook based on the activities of the user on Facebook, or to stop appearing in social ds. This amounts to an 'opt-out' mechanism, which according to the Article 29 Working Party 'is not an adequate mechanism to obtain average users' informed consent', especially in respect of behavioural advertising.[290] Worse still, it is not possible to opt-out from specific types of advertising, such as Sponsored stories.

Nor is it possible to stop sharing location data with Facebook. When it comes to sharing location data with Facebook, users only have a binary choice: all or nothing. Once the Facebook mobile app is authorized to access location data, there are no further (in-app) settings, for example, allowing the individual to authorise location sharing for one purpose but decline it for other purposes. In addition, whilst Facebook is to some extent explicit about the types of information it collects in order to locate its user, the description of the purposes for which it does so is unsatisfactory.[291] Facebook should offer granular in-app settings for sharing of location data, with all parameters turned off by default. This should allow users to determine when, how and what type of (location) data can be used by Facebook and for what purpose. Additionally, Facebook should provide more detailed information about exactly how, when and why location data is collected. Finally, location data should only be collected to the extent and for the duration necessary for the provision of a service requested by the user.

In view of the above, the consent Facebook elicits from its users to process their personal data, including the processing of data enabled by Facebook's exploitative terms, is neither

[288] ibid 24.
[289] Facebook, '2018 Data Policy' (n 241).
[290] Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010) 15.
[291] Facebook informs: 'For example, we use information collected about your use of our Products on your phone to better personalise the content (including ads) or features that you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad that we showed you on your phone on a different device.' Facebook, '2018 Data Policy' (n 241).

freely given, specific, informed nor unambiguous, and therefore Facebook systematically processes its users' personal data in violation of the GDPR.

4. Degradation of Quality

It has been shown that the terms assessed in Section III.A.1 are exploitative because users have no choice but to agree to them to access the services of the dominant provider of the social networking services. As a result, users suffer the loss of control over their personal data, as they cannot control how this data is used and combined, not least because 'Facebook's users are oblivious as to which data from which sources are being merged to develop a detailed profile of them and their online activities.'[292]

Furthermore, the argument has been made that privacy harms can be equated to a reduction in the quality of a good or service, which is a standard category of harm that results from market power.[293] Commenting on the Google/DoubleClick merger, Swire asserted that the merger would entail the combination of Google's 'deep' information about an individual's actions, such as detailed information about search terms, with DoubleClick's 'broad' information about an individual's actions, such as the surfing behaviour of an individual after leaving Google, and that this combination of 'deep' and 'broad' information 'may be a significant reduction in the quality of the search product' for the 'many millions of individuals with high privacy preferences.'[294] Therefore, if reduction of product quality is an effect actionable under competition law and consumers regard privacy as an aspect of product quality, reductions of privacy protection should be taken as consumer harm in competition assessments. The problem of this argument lies in the 'significant, yet elusive nature of quality'.[295] Whilst it is acknowledged that in many cases quality is more important than price as a competition parameter, defining and measuring quality is a daunting task,[296] especially given that consumers have different appreciations of what quality is.

However, this measurement problem can be solved by reference to the data protection regime. In competition analysis, it is possible to consider that a deterioration of the terms under which a dominant provider of a data-driven service protects its users' personal data, and therefore a reduction of the quality of its service, is harmful to consumers, but competition law lacks the 'normative tools' to determine what exactly is low or reduced quality.[297] Yet, competition law can borrow this normative judgment from the data protection regime, given that it provides a framework for judging whether the processing of personal data is acceptable or unacceptable.[298] As the *Autorite de la Concurrence* and the *Bundeskartellamt* observe 'looking at excessive trading conditions, especially terms and conditions which are imposed on consumers in order to use a service or product, data

---

[292] Bundeskartellamt (n 88) 4.
[293] Peter Swire, 'Protecting Consumers: Privacy Matters in Antitrust Analysis' (*Center for American Progress*, 2007) <https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/>.
[294] ibid.
[295] Ariel Ezrachi and Maurice E Stucke, 'The Curious Case of Competition and Quality' [2014] University of Tennessee Legal Studies Research Paper No. 256 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494656##>.
[296] ibid 1.
[297] Francisco Costa-Cabral and Orla Lynskey, 'The Internal and External Constraints of Data Protection on Competition Law in the EU' [2015] LSE Law, Society and Economy Working Papers 25/2015 17.
[298] ibid 18.

privacy regulations might be a useful benchmark to assess an exploitative conduct.'[299] In particular, a data protection infringement can be a clear normative signal of lower quality, given that '[if] a dominant undertaking exploitatively reduces the quality of its data […] policy, consumers will be worse off than had competitive levels prevailed, which […] must normatively be set at compliance with data protection law.'[300]

For over 10 years Facebook only processed its users' personal data collected on Facebook for advertising purposes, and when it attempted to expand the scope of its data collection practices to external websites and apps, its users complained and disapproved of that initiative, forcing Facebook to abort that attempt.[301] But when Facebook was finally freed from competitive pressure, it included in its Data Policy a number of terms that enabled it to track users off Facebook and combine their data collected from myriad sources to enrich its user profiles and improve its ad targeting technology, terms which, as seen above,[302] infringe data protection law. Accordingly, not only were Facebook users exploited as a result of the elimination of consumer choice, loss of control over their personal data and violation of their data protection rights, but they also suffered the quality degradation of their social networking experience.

Given that the objective of Facebook's exploitative terms was to collect more personal data for consumer profiling[303] and thereby strengthen its position in the display advertising market, the reduction of competition on this side of Facebook's multisided market is directly correlated to a degradation of quality on the user side.

B. Data Privacy Violations and Deception to Exclude Competing Social Networks and Providers of Display Advertising

Given the strong causation between access to greater volumes of data and enhanced quality of data-driven products and services,[304] Facebook's ability to gather more data than its competitors in the social network and display advertising markets has been decisive to the attainment and later strengthening of its dominant position. There is nothing wrong with being able to gather more data than your competitors when this ability is the result of competition on the merits. For example, through the introduction of new innovative features that prove popular amongst users[305] and therefore lead to more engagement, traffic and ultimately more data. However, when an undertaking uses 'unfair tactics to attain or maintain its dominant position, then […] using the valuable consumer data from its illegally maintained or attained monopoly is not competition on the merits.'[306]

Violations of data privacy and deception to enable and conceal such violations have been the two main weapons that Facebook has wielded to gain a data-driven competitive advantage and attain[307] and reinforce[308] its dominant position. In particular, such unlawful

[299] Autorité de la Concurrence and Bundeskartellamt (n 213) 25.
[300] Costa-Cabral and Lynskey (n 298) 21.
[301] See text accompanying footnote 149.
[302] See Section III.A.3.
[303] The lower the data protection levels, the richer the consumer profiles and the higher the advertising revenues. See text accompanying footnote 256.
[304] See Section I.C.2.
[305] Such as Snapchat's Stories, which Facebook blatantly ripped off. See text accompanying footnote 495.
[306] Stucke and Grunes (n 25) 291.
[307] See Sections II.C.2 and II.C.3.
[308] See Section III.A.3.

behaviour has given Facebook access to more data to improve its services and attract more users and advertisers to its network, thereby increasing the quality gap between its stack of products and services and that of its competitors, and reducing the incentives of the latter group to compete and innovate.[309] This unlawful behaviour amounts to an abuse within the meaning of Article 102(b) TFEU.

It is acknowledged that an abuse of this type is novel. However, when determining whether conduct that does not fall squarely within any established category of abuse amounts to an abuse of a dominant position, the EU courts assess (i) whether the conduct at issue falls within the scope of competition on the merits, and if it does not; (ii) whether actual or potential anticompetitive effects can be shown.[310] As a matter of fact, that was the approach followed in *AztraZeneca,*[311] where the EU Courts had to determine whether specific behaviour consisting of the misuse of the patent system, not previously considered in EU case law, infringed Article 102 TFEU.[312] Noting that Article 102 TFEU bans dominant undertakings from eliminating competition through 'methods other than those which come within the scope of competition on the merits',[313] the CJEU held that having recourse to highly misleading representations in order to lead public authorities into error (for the purposes of improperly obtaining exclusive rights) was 'manifestly not consistent with competition on the merits and the specific responsibility on such undertaking not to prejudice, by its conduct, effective and undistorted competition.'[314] The CJEU concluded that it was an abuse 'to lead the public authorities [to] wrongly […] create regulatory obstacles to competition, for example by the unlawful grant of exclusive rights to the dominant undertaking.'[315] However, the CJEU also held that this conduct, in and of itself,

[309] The existence of anticompetitive behaviour based on the violation of privacy and deceit is becoming acknowledged. See for example OECD, "'Big Data: Brining Competition Policy to the Digital Era'" (2016) §"Once example requiring the attention of the competition authority is where the privacy violation is reasonably capable of helping a company attain or maintain its monopoly power (especially in markets with strong data-driven network effects). ; Eric Clemons, 'Written Evidence Submitted to the House of Lords for the Report "Online Platforms and the Digital Single Market"' <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online-platforms-and-the-eu-digital-single-market/written/25630.html.>"[S]ome anti-competitive activities are subsidized through revenues gained through violation of privacy law […] rather than through violation of competition law itself." ; Anca D Chirita, 'The Rise of Big Data and the Loss of Privacy' [2016] Durham Law School Research Paper"This paper acknowledges that a potential misuse of personal data by dominant undertakings has no precedent line of case law. While its novelty could trigger this particular form of abuse to be affixed with an exotic label, as it sits outside the confines of traditional competition practice under Article 102 TFEU, it is never to be under-estimated by dominant undertakings that actively engage in the sharing, transferring, or selling of such data". ; Stucke and Grunes (n 25) 155"Companies may use traditional measures (such as mergers, tying, exclusive dealing) to maintain or attain market power. Dominant firms may engage in otherwise illegal practices (such as deceiving the public on their privacy policies) or violating citizens' legal rights regarding the privacy of their personal data"; '[T]he rules of fair competition and the privacy rules can be violated by [...] commercial operations on the internet. Companies with market power can use this kind of conduct to entrench their market position' Monopolkommission, 'Special Report 68: Competition Policy: The Challenge of Digital Markets' (2015) 117 <http://www.monopolkommission.de/index.php/en/reports/special-reports/284-special-report-68>.

[310] Alison Jones, 'Standard-Essential Patents: FRAND Commitments, Injunctions and the Smartphone Wars' (2014) 10 European Competition Journal 1, 21.

[311] *Case C-457/10 P, AstraZeneca v Commission [2012] ECLI:EU:C:2012:770*.

[312] Jones (n 311) 21–22.

[313] *Case C-457/10 P, AstraZeneca v Commission [2012] ECLI:EU:C:2012:770* (n 312) para 75.

[314] *ibid 98*.

[315] ibid 105.

was not enough to constitute an abuse; rather, actual or potential anticompetitive effects were required.[316]

Facebook's privacy-intrusive and deceptive conduct does not constitute competition on the merits (1) and leads to actual anticompetitive effects (2).

1. Departure from Competition on the Merits

In *Post Danmark I,* the CJEU held:

> 'Article [102 TFEU] applies, in particular, to conduct of a dominant undertaking that, through recourse to methods different from those governing normal competition on the basis of the performance of commercial operators, has the effect, to the detriment of consumers, of hindering the maintenance of the degree of competition existing in the market or the growth of that competition.'[317]

The concept of 'competition on the merits' has been widely criticised for being too vague and devoid of substantive meaning.[318] However, one discerning line to narrow down the types of conduct that are admissible to protect a dominant firm's commercial interest is the violation of other laws that leads to a competitive advantage and the foreclosure of competition.[319] Facebook, in particular, has infringed EU data protection (i) and consumer protection law (ii) to this end.

(i) EU Data Protection Law

It was seen in Section III.A that Facebook included in its Data Policy unfair trading conditions that infringe EU data protection law with an aim to expand the scope of its data processing operations to enrich its user profiles and improve its ad targeting algorithms, thereby reinforcing its position in the display advertising market. This behaviour falls outside the scope of competition on the merits, since through the violation of data protection law Facebook has fuelled network effects and data-driven externalities, and consequently enhanced the effects of its virtuous cycle,[320] thereby foreclosing competitors in the social network and display advertising markets that cannot match Facebook's scale and unparalleled access to data.

For example, the Brussels Court of First Instance recently held that Facebook's tracking of people outside Facebook with the aid of Social Plugins such as the 'Like' button and

---

[316] The CJEU held that the anticompetitive effect 'does not necessarily have to be concrete, and it is sufficient to demonstrate that there is a potential anti-competitive effect (see to that effect TeliaSonera Sverige, paragraph 64).' ibid 112.
[317] *Case C-209/10, Post Danmark A/S v Konkurrenceradet (Post Danmark I) [2012] ECR I-0000* paras 22–24.
[318] Wolf Sauter, *Coherence in EU Competition Law* (Oxford University Press 2016) 110–111; Ekaterina Rousseva, 'The Concept of 'Objective Justification'of an Abuse of a Dominant Position: Can It Help to Modernise the Analysis under Article 82 EC' (2006) 2 The Competition Law Review 27, 30.
[319] 'An exclusionary abuse might equally be based on a data protection infringement: dominant undertakings are also under a special responsibility to only resort to "competition on the merits" and a data protection infringement represents a departure from such competition on the merits.' Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 11, 35.
[320] See Section I.C.3.

other trackers is illegal, and that its approach to consent is invalid.[321] The Court noted that the data Facebook receives from its social plug-ins installed on websites (which includes IP address, URL of the page of the website requested by the user, the browser management system, the type of browser and cookies)[322] is 'frequently of a very sensitive nature, allowing, for example, health-related, sexual and political preferences to be gauged'.[323] In addition, the Court observed that Facebook's widespread presence across the web renders this tracking 'practically unavoidable',[324] and that 'the extent of the violations in question is massive: they do not only concern the violation of the fundamental rights of a single person, but of an enormous group of persons.'[325] Moreover, the Court held that Facebook's request for consent was not specific, for which reason any consent it received was unlawful.[326] Also, Facebook did not provide sufficient information about the 'purposes' for which Facebook processes the personal data,[327] and did not provide information about 'the existence of a right to access and correction of the personal data concerning [users].'[328] These data protection infringements logically resulted in the violation of Belgian Internet users' fundamental right to data protection. However, at the same time, they enabled Facebook to gather and process detailed personal data about 'innumerable internet users in Belgium'[329] to fuel data-driven economies and network effects. As the *Autorite de la Concurrence* observes, 'data collection and mining can intensify network effects when the increase in the number of users of a company enable it to gather more data than its competitors and increase the quality of its products or services and ultimately its market share.'[330]

(ii) EU Consumer Protection Law

In the social network market there is a significant informational gap between Facebook and consumers. Whilst Facebook knows everything about the data processing practices in which it engages, their impact on users' data privacy and the value it can derive from data, some consumers struggle even to understand what a privacy policy is. For example, in one study 65% of the participants did not know that the statement '[w]hen a website has a privacy policy, it means that the site will not share my information with other websites and companies without my permission' is false.[331] Accordingly, when contracting with Facebook, consumers are placed on 'the less advantageous side of an agreement formed and executed with asymmetric information.'[332] Information asymmetries commonly lead to consumers making transactional decisions contrary to their interests. For example, a given user may have a declared preference for privacy-driven services, but if he sticks to a default option in privacy or ad settings and lacks the necessary understanding of the privacy

[321] *Willem Debeuckelaere v Facebook Ireland Ltd, and Facebook Inc, and Facebook Belgium Bvba 2016/153/A* (Dutch-language Brussels Court of First Instance).
[322] ibid 9.
[323] ibid 69.
[324] ibid.
[325] ibid.
[326] ibid 61.
[327] ibid 58.
[328] ibid 59.
[329] ibid 69.
[330] Autorité de la Concurrence, 'Opinion No. 18-A-03 of 6 March 2018 on Data Processing in the Online Advertising Sector' (2018) 52–53 <http://www.autoritedelaconcurrence.fr/doc/avis18a03_en_.pdf>.
[331] Joseph Turow, Michael Hennessy and Nora A Draper, 'The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation' (2015) A Report from the Annenberg School for Communication, University of Pennsylvania 4.
[332] Jan Whittington and Chris Jay Hoofnagle, 'Unpacking Privacy's Price' (2012) 90 N. C. L. Rev. 1327 1341 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2059154>.

implications arising from this choice, his poor understanding benefits the service provider (as he is unwittingly providing his personal data) and prevents him from actually protecting his privacy.

Aware of consumers' privacy preferences but driven by an insatiable appetite for personal data, Facebook has deliberately limited the visibility of the data processing practices associated with the use of its social networking services and has engaged in otherwise deceptive practices in a move to reinforce information asymmetries.

To understand the privacy implications of using Facebook, consumers must read Facebook's Data Policy. But Facebook's Data Policies over the years have been progressively designed to impair consumer's ability to accurately and thoroughly understand Facebook's data processing practices, as they have increasingly become lengthier, more complex, more difficult to navigate and more vague. Indeed, in a study of Facebook's privacy policies from 2005 to 2015, Shore and Steinman found that '[t]he measure of whether Facebook's privacy policy fully describes use of Internet monitoring technologies, including but not limited to beacons, weblogs, and cookies, dropped from 4 to 0'.[333] 0 indicating that the privacy policy did not meet the criteria of the Patient Privacy Rights framework to assess a privacy policy's ability to inform users about a company's data processing practices, and 4 indicating that the criteria are fully met.[334]

Currently, Facebook's Data Policy, excluding the additional links to separate webpages, is almost 4,500 words,[335] and would take an average reader between 10 and 20 minutes to read.[336] Moreover, the language of Facebook's Data Policy is complex, which makes it harder for average consumers to process the information it contains.[337] Further, Facebook's Data Policy is vague with regards to its data collection, use and disclosure practices, often relying on the words 'may'[338] or 'can'. The use of the words may and can gives Facebook significant discretion to do, or not do, the actions prefaced by those words, and consumers reading its Data Policy consequently cannot accurately determine the exact scope of the data Facebook is collecting from them or how that data will be used and disclosed.[339] This is inconsistent with consumer preferences.[340] Indeed, the UK Competition Markets Authority (the CMA) has confirmed that 'consumers want more transparency and clearer explanations of how their data will be used before they consent to its collection.'[341] Lastly, Facebook's Data Policy is hard to navigate, containing over 70 links to other pages. The interlinking of separate pages dramatically increases the amount

[333] Jennifer Shore and Jill Steinman, 'Did You Really Agree to That? The Evolution of Facebook's Privacy Policy' [2015] Technology Science </a/2015081102/>.
[334] ibid.
[335] Facebook, '2018 Data Policy' (n 241).
[336] Australian Competition & Consumer Commission, 'Digital Platforms Inquiry - Preliminary Report' (2018) 183.
[337] ibid.
[338] For example, Facebook's DP states: 'Apps and websites that you use may receive your list of Facebook friends.' Similarly, 'When you choose to use third-party apps, websites or other services that use, or are integrated with, our Products, they can receive information about what you post or share'. Facebook, '2018 Data Policy' (n 241); Additionally, we may use cookies to remember your choices, like your language preferences, to provide a safer experience, and otherwise to customize our Services for you. WhatsApp, 'WhatsApp Privacy Policy' (*WhatsApp.com*) <https://www.whatsapp.com/legal/?eea=1#privacy-policy-information-we-collect>.
[339] Australian Competition & Consumer Commission (n 337) 183.
[340] See Section II.A.
[341] CMA, 'The Commercial Use of Consumer Data – Report on the CMA's Call for Information' (2015) 138.

of navigation and reading time for a user, as there is commonly no differentiation between links that contain key terms and links that contain explanatory content.[342] For example, under 'Information from partners' on Facebook's 2018 Data Policy, one of the links is 'learn more', which takes the reader to a page containing more information about the third-party data providers with whom Facebook shares user data, although there is no additional information on how and with whom those data providers can further share user data.[343] Therefore, Facebook's 2018 Data Policy exacerbates the information asymmetries between Facebook and consumers by providing consumers with an opaque view of its data processing practices whilst simultaneously setting out broad discretions to collect, use and disclose users' personal data.

In addition, Facebook elicits user consent to its data practices in response to a 'clickwrap agreement', which is a 'digital prompt that facilitates consent processes by affording users the opportunity to quickly accept or reject digital media policies'.[344] As a result, users are steered away from Facebook's Data Policy that might encourage dissent and are kept 'in fast lanes to monetized sections of services'.[345] The use of clickwrap agreements by Facebook means that users signing up are required to agree to its Governing Documents, which include extensive rights to collect, use and disclose user data, without being asked to actually review any of them. Use of these agreements by Facebook contributes to the tendency of consumers not to read online terms of service and privacy policies, thereby reinforcing information asymmetries between consumers and Facebook with regard to the legal terms of their relationship. Moreover, Facebook's clickwrap agreement is presented to consumers on a take-it-or-leave-it basis, which means that consumers are presented with a standard set of terms that are offered to all prospective users with no opportunity to negotiate any specific term, including with regard to how much personal data can be collected or how it may be used and shared with third parties. The use of take-it-or-leave-it terms is a depiction of the significant bargaining power held by Facebook vis-à-vis consumers, since Facebook can unilaterally set the terms applicable to its transactions with consumers, which include the right to unilaterally change its Governing Documents from time to time. Conversely, consumers are only able to decide whether or not to consent to the entirety of Facebook's Governing Documents to access its services.

Furthermore, Facebook's privacy settings are deceptive. Whilst they offer users significant control regarding access to their data by other Facebook users, the same cannot be said in respect of the collection and use of data by apps, websites and Facebook. For example, whilst users can control who sees what they post in the News Feed and on their profile, who sees their contact phone and email address, and who sees the apps and websites they use, if all advertising data sharing settings are turned off, third parties may still target advertising on Facebook to users based on things that users do on Facebook, third parties may still use contact information to match their customer list to a Facebook profile and target advertising to that user, and there is no setting that prevents Facebook from targeting advertising to users while on Facebook based on the apps and websites they use.[346] Similarly, as noted above,[347] there are no options to stop sharing location data with

[342] Australian Competition & Consumer Commission (n 337) 183.
[343] Facebook, 'How Does Facebook Work with Data Providers? | Facebook Help Centre' <https://www.facebook.com/help/494750870625830?ref=dp>.
[344] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media' (2018) 4 Social Media+ Society 1.
[345] ibid.
[346] Australian Competition & Consumer Commission (n 337) 207.
[347] See paragraph containing footnote 291.

Facebook. Consequently, 'users are able to choose from several granular settings which regulate access by other individuals, but cannot exercise meaningful control over the use of their personal information by Facebook or third parties. This gives users a false sense of control.'[348]

Moreover, Facebook has designed user interfaces that lead consumers to make privacy-intrusive selections, including the use of default setting to opt-in users to certain types of data collection or the use of choices preselected in ways that nudge users toward more privacy-intrusive choices. The nudge is made by appealing to behavioural biases such as for example the default and status quo effect and preference for ease.

For instance, it has been proved over and over again that most users never look at, let along change, the default settings.[349] Accordingly, when the default settings allow for widespread collection and use of personal data, users are nudged towards giving away their data, and they are unlikely to change this option. For example, the Facebook GDPR popup required users to go into 'Manage data settings' to turn off ads based on data from third parties. If a user simply clicked 'Accept and continue', the setting was automatically turned on.[350]

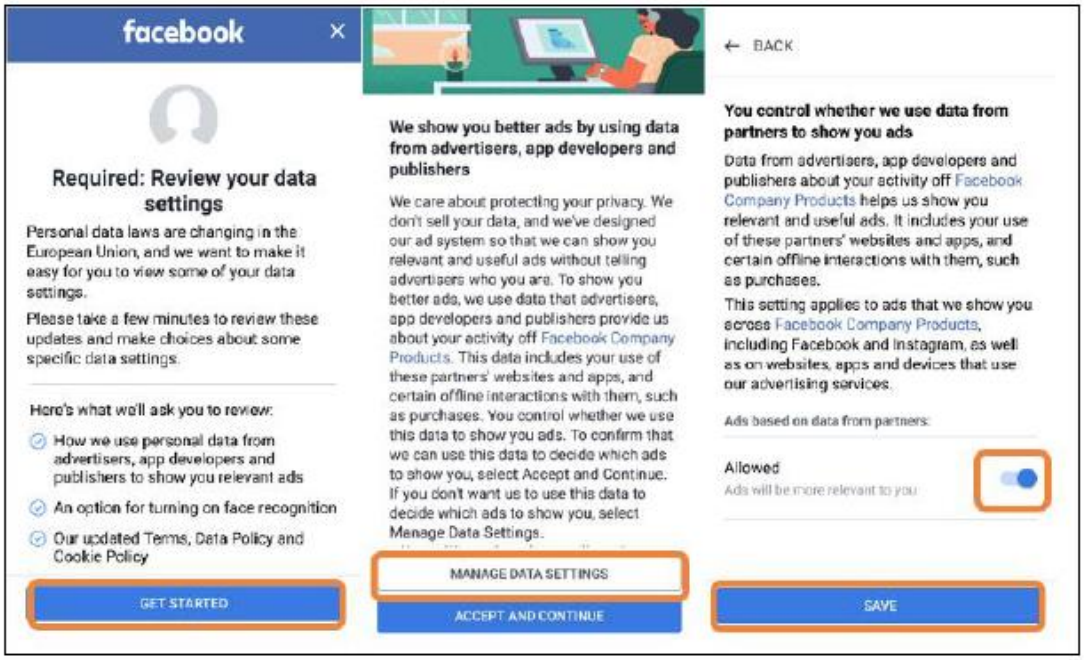

Figure 2: Facebook's GDPR pop-up window

In fact, the Norwegian Consumer Council (Forbrukerrådet) recently found that Facebook has 'default settings preselected to the least privacy friendly options'.[351] This is highly

[348] Brendan Van Alsenoy and others, 'From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms' (2015) Report commissioned by the Belgian Data Protection Authority 22.
[349] Jared Spool, 'Do Users Change Their Settings?' (November 2011) <https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/>.
[350] Norwegian Consumer Council (Forbrukerrådet), 'Deceived by design' (2018) 14 <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/>.
[351] ibid 15.

concerning, as 'the default setting of whether data are immediately shared or not probably has more effect [on disclosure of data] than any other issue of design.'[352]

Relatedly, on Facebook's GDPR-popup, the interface was designed with a bright blue button enticing users to 'Accept and continue.' Taking the easy path by clicking this button would take the user to a new screen about face recognition, with equivalent similar button to accept and continue. Conversely, users who wanted to limit the data Facebook collects and how it uses it, had to first click a grey box labelled 'Manage data settings,' where they were led through a long series of clicks in order to turn off 'Ads based on data from partners' and the use of face recognition technologies. This path was, in other words, considerably longer. Users that were in a rush to use Facebook were inclined to simply click the blue button and be done with the process, which results in the maximum amount of data collection and use. This 'easy road' consisted of four clicks to get through the process, which entailed accepting personalised ads from third parties and the use of face recognition. In contrast, users who wanted to limit data collection and use had to go through 13 clicks.[353] By making it simpler and more streamlined to allow the collection of the largest amount of data, in comparison to limiting data sharing, Facebook was nudging users toward the former.[354]

According to the Directive on Unfair Commercial Practices, a commercial practice is misleading when it 'contains false information and is therefore untruthful or *in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct*, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise'.[355] As seen above,[356] some consumers are concerned about the protection of their personal data, and want more control over it. Privacy-sensitive users are likely to read Facebook's Data Policy to understand and perhaps mitigate any potential privacy harms that may ensue from using Facebook's services, and to make a decision as to whether or not to sign up or stick to default options. However, their transactional decisions may be made based on a poor understanding of Facebook's long, complex, vague and difficult to navigate Data Policy, carefully designed interfaces that nudge consumers to stick to the most privacy-intrusive settings, as well as by a false sense of control over their personal data motivated by misleading privacy settings. By presenting information in a way that is capable of deceiving the average consumer, and by giving users a false sense of control over their personal data, Facebook engages in misleading commercial practices. Additionally, by not providing and/or providing in an unclear and ambiguous manner material information that consumers need to take an informed transactional decision, thereby causing or being likely to cause consumers to take a transactional decision that they would not have taken otherwise,[357] Facebook effects misleading omissions.[358]

---

[352] Jamie Bartlett in House of Lords (n 33) 32.
[353] Norwegian Consumer Council (Forbrukerrådet) (n 351) 20.
[354] ibid.
[355] Article 6(1) Unfair Commercial Practices Directive. Emphasis added.
[356] See Section II.A.
[357] See Article 7(2) Unfair Commercial Practices Directive.
[358] Indeed, according to the Commission, 'the use of defaults (choices consumers are presumed to make unless they expressly indicate otherwise) or the provision of unnecessarily complex information may, according to the circumstances of the case, prove misleading.' European Commission, 'Unfair Commercial Practices Guidance' <https://webgate.ec.europa.eu/ucp/public/index.cfm?event=public.guidance.browse&Article=Article-62&elemID=74#Article-62>.

As a result of Facebook's misleading commercial practices and omissions, some consumers are deterred from attempting to become informed on the privacy implications of using Facebook. Overwhelmed by the amount of complex, difficult-to-find and vague information contained in Facebook's Governing Documents, some users prefer to remain in blissful ignorance ('ignorant consumers'). At the same time, said practices and omissions preserve and enhance consumer confusion with regard to data privacy concerns arising from using Facebook. They give a false sense of control over the ability of users to choose which type of personal data Facebook or third parties may or may not collect, process and share, and lead consumers to have a mistaken undertaking, motivated by deceit, of Facebook's data processing activities. For example, users may wrongfully believe that a given privacy setting prevents the collection and processing of their personal data for display advertising, in circumstances where it only prevents the use of that data for display advertising on websites and apps outside Facebook, or may be induced to stick to privacy-intrusive settings that are inconsistent with their privacy preferences ('confused consumers').

A high number of ignorant and confused consumers explain the interesting phenomenon that took place in November 2012 when Facebook announced an update to its Data Policy and Statement of Rights and Responsibilities. Soon after the announcement, millions of users posted and shared with friends a statement[359] that aimed to protect their personal information that users now saw threatened by the new update, which was of course ineffective from a legal standpoint and denoted most Facebook users' lack of any understanding whatsoever of Facebook's Governing Documents. The notice went 'viral', for which reason it was largely covered by the media.[360] However, some of the most crucial changes of the update were the ability of Facebook to share its users' data with its 'Family companies' and the proposal to revoke users' right to vote on future policy changes that

[359] The statement read as follows: 'In response to the new Facebook guidelines I hereby declare that my copyright is attached to all of my personal details, illustrations, comics, paintings, professional photos and videos, writings, and expressions of all kinds, as my sole and exclusive intellectual property, as defined in the Berne Convention, and by US law, custom, and practice.. For commercial use of the above, my written consent is needed at all times and for all reasons, without exceptions. (Anyone reading this can copy this text and paste it on their Facebook Wall. This will place them under protection of copyright laws.) By this publishing, and henceforth forever, I notify Facebook that it is strictly forbidden to disclose, copy, distribute, disseminate, or take any other action against me on the basis of this profile and/or its contents. The aforementioned prohibited actions also apply to employees, students, agents and/or any staff under Facebook's direction or control. The content of this profile is private and confidential information. The violation of my privacy is punished by law (UCC 1 1-308-308 1-103 and the Rome Statute), and such other national and international laws and treaties as may apply, and by tort and common law.' Jeff Bercovici, 'That Facebook Copyright Protection Notice Is An Urban Myth' (*Forbes*, 26 November 2012) <https://www.forbes.com/sites/jeffbercovici/2012/11/26/that-facebook-copyright-protection-notice-is-an-urban-myth/>.

[360] Brittany Darwell, 'Fake Facebook Copyright Notice Goes Viral as Actual Data Use Policy Is up for Review' (26 November 2012) <https://www.adweek.com/digital/fake-facebook-copyright-notice-goes-viral-as-actual-data-use-policy-is-up-for-review/>; Dave Thier, 'Why You Can't Protect Your Facebook Privacy With A Wall Post' (*Forbes*, 26 November 2012) <https://www.forbes.com/sites/davidthier/2012/11/26/why-you-cant-protect-your-facebook-privacy-with-a-wall-post/> accessed 19 April 2019; Erin Griffith, 'The Facebook Legal Notice Meme Is Hilarious and Scary (for Facebook)' (*Pando*, 26 November 2012) <https://pando.com/2012/11/26/the-facebook-legal-notice-meme-is-hilarious-and-scary-for-facebook/>; Kevin Smith, 'Don't Post This Bogus Copyright Message On Your Facebook' (*Business Insider*, 26 November 2012) <https://www.businessinsider.com/bogus-facebook-copyright-message-2012-11>; Hubert Nguyen, 'Facebook Privacy Message Is Pointless. Stop Posting' (*Ubergizmo*, 26 November 2012) <https://www.ubergizmo.com/2012/11/facebook-privacy-message-is-pointless-stop-posting/>; Scott Ross, 'Mark Zuckerberg Is Not Trying to Steal Your Copyrights' (*NBC Bay Area*, 26 November 2012) <http://www.nbcbayarea.com/news/tech/Facebook-Mark-Zuckerberg-Copyrights-180861911.html>.

Facebook had introduced in 2009 to calm the uprising caused by privacy scandals in that year.[361] Given that such right was still in effect, the update was put for vote. 589,141 users (87.5 per cent) opposed to the changes, whilst 79,731 supported them. Had Facebook users posting and sharing the statement above read and understood the policy update, the voter turnout would have been significantly higher. However, the complexity of Facebook's Governing Documents deterred the average consumer from engaging with and understanding the update. The result of the referendum was ultimately unenforceable, as according to Facebook's terms the participation of 30 per cent of Facebook's users (then 300 million) was required for the result to be upheld.[362]

As will be seen in the next Section, a high number of ignorant and confused consumers raises barriers to entry and distorts competition in the social network market.

2. Actual Anticompetitive Effects

In *Deutsche Telekom*, the CJEU held that actual or likely anticompetitive effects must relate to the possible barriers which the dominant firm's practices may create to the maintenance of the degree of competition existing in the relevant market or markets or the growth of that competition.[363] Facebook's violations of data protection and consumer protection law above have significantly raised barriers to entry in the markets for social networks and display advertising and reduced the degree of competition therein.

In particular, the imposition of unfair trading conditions has given Facebook access to large volumes of additional personal data to improve its social and ad targeting algorithms, thereby fuelling its virtuous cycle. In turn, by deepening information asymmetries through misleading commercial practices and omissions, Facebook obfuscates its data processing operations in such a way that only a limited number of consumers duly understand the fact that data collection and processing is taking place, as well as its magnitude and potential detrimental effects on online privacy (i.e. 'sophisticated' consumers,[364] as opposed to 'ignorant' and 'confused' consumers). A high number of ignorant and confused consumers relative to sophisticated consumers brings about two important benefits for Facebook, to the detriment of competition. First, a high portion of its users is likely to unwittingly share their personal data in a manner contrary to their privacy preferences based on deceit or a poor understanding of Facebook's data processing practices, interfaces and privacy settings, with which Facebook is able power its virtuous cycle even further. Second, sophisticated consumers are compelled to stick to Facebook due to the operation of strong direct network effects,[365] in spite of their awareness of Facebook's privacy-intrusive practices.

The strategy and effects above greatly raise barriers to entry in the two-sided market for social networking services and display advertising. A newcomer can choose entering the market either based on a data-driven, advertising-based business model (such as Facebook's) or a privacy-friendly one (such as WhatsApp's prior to its acquisition by

---

[361] See text accompanying footnote 151.
[362] Dan Farber, 'The Facebook Vote and a Nation-State in Cyberspace' (*CNET*, 11 December 2012) <https://www.cnet.com/news/the-facebook-vote-and-a-nation-state-in-cyberspace/>.
[363] *Case C-280/08 P, Deutsche Telekom AG v Commission [2010] ECR I-9555* [252].
[364] Georg Clemens and Mutlu Özcan, 'Obfuscation and Shrouding with Network Effects: Big Data Strategies and the Limits of Competition' [2017] SSRN paper 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3023467>.
[365] ibid 5.

Facebook). In the former case the entrant would face high barriers to entry in the form of strong direct and indirect network effects and data-driven economies powered by Facebook's exploitative terms and misleading practices. In the latter case the entrant will realise that its business model has no appeal for the majority of Facebook users (given that ignorant and confused consumers do not perceive any benefit from its privacy-friendly proposition as a consequence of Facebook's misleading practices and omissions), and that lock-in resulting from 'everybody being on Facebook' prevents switching by sophisticated consumers. In both cases the outcome is the same: the entrant cannot successfully achieve critical mass to be viable, for which reason Facebook ends up being completely insulated from competitive pressure on the user side, which in turns protects its position of leadership on the advertiser side.

Competition in the social network market was already poor on the date the 2015 Data Policy came into force, which through the imposition of exploitative terms, gave Facebook access to additional personal data about its users to improve its algorithms. However, since that date the competitive landscape in this market has deteriorated significantly. This is because the merging of data enabled by the exploitative terms[366] enhances direct network effects and consequently 'the "locking-in" of users […], to the detriment of other providers of social networks.'[367] Indeed, Facebook's monthly active users (MAU) went from 1.39 billion as of December 2014 to 2.32 billion as of December 2018, and its daily active users (DAU) from 890 million on average for December 2014 to 1.52 billion on average for December 2018.[368] Facebook's current closest competitor is Instagram, which Facebook controls, with 1 billion MAU and 500 million DAU in 2018.[369] Importantly, Google+ began its exit from the market in April 2019.[370] Other social networks such as LinkedIn, SnapChat and Twitter do not exert meaningful competitive pressure on Facebook, as they serve a complementary need from the users' perspective,[371] and therefore are not adequate substitutes.

Actual anticompetitive effects are apparent in the display advertising market. Display advertising is the main source of income of content publishers, especially media and news websites and apps, and therefore they compete with Facebook on this side of the market. The exploitative terms introduced in the 2015 Data Policy harmed publishers to a great extent, given that by enabling Facebook's surveillance of their readers and visitors, Facebook was able to undercut their value and publishers' pricing power over them.[372] For example, a website publisher such as the TechCrunch attracts a well-defined audience interested in gadgets, technology and Internet trends. The TechCrunch has an interest in keeping that audience engaged with its website, so it can show its audience ads that are targeted to their interests and thereby make profits when users click on an ad. However,

---

[366] That is, the merging of data collected from Facebook, Instagram, WhatsApp and third party websites and apps using Facebook's technologies and advertising services.
[367] Bundeskartellamt (n 88) 4.
[368] See Forms 10-K "Annual Report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934" for the fiscal years ending on 31 December 2014 to 31 December 2018, filed by Facebook with the U.S. Securities and Exchange Commission, available at https://www.sec.gov/cgi-bin/browse-edgar?company=facebook&owner=exclude&action=getcompany
[369] Omnicore Agency, 'Instagram by the Numbers (2019): Stats, Demographics & Fun Facts' (4 January 2019) <https://www.omnicoreagency.com/instagram-statistics/>.
[370] Chris Welch, 'Google Begins Shutting down Its Failed Google+ Social Network' (*The Verge*, 2 April 2019) <https://www.theverge.com/2019/4/2/18290637/google-plus-shutdown-consumer-personal-account-delete>.
[371] Bundeskartellamt (n 88) 3.
[372] Srinivasan (n 138) 64.

the ability to monitor Internet users arising from the introduction of the exploitative terms meant that Facebook could determine with precision who the members of the TechCrunch actually are, follow them throughout the Internet and target them with ads on any website or app other than the TechCrunch, charging a significantly lower ad serving cost than that the TechCrunch would charge. As Srinivasan explains, 'if Facebook could compile a list of people that read the *Journal*, even those who did not use Facebook, it could simply sell the ability to retarget "*Journal* readers" with ads across the internet for a fraction of the cost that the *Journal* charged.'[373] Put in other words, Facebook contributed to the commoditisation of publishers' most valued asset: their loyal audiences.

Decreasing revenues for news publishers in turn lead to negative externalities that are worth mentioning. It has been widely documented that news publishers have been adversely affected by changes in news consumption (i.e. from offline to online consumption) and a steep decrease in print advertising. [374] To remain profitable, news publishers in the US, Canada, Australia and across Europe have had to cut back the breadth and depth of their news reporting service and invest less in good quality journalism,[375] including investigations into abuses of power in the public and private spheres and the daily activities of public institutions, which are particularly high-cost and risky.[376] Low rates of production of this type of journalism has a negative impact on democracy, since there is less information to the public about political issues, which is linked to lower engagement by the public in the political process.[377]

In addition, the additional data that Facebook is able to amass as a result of its exploitative terms and deceiving behaviour enables it to enrich its user profiles and therefore refine its ad-targeting capabilities, to the detriment of content publishers[378] and other suppliers of display advertising like Twitter and Snapchat that cannot match Facebook's unparalleled audience and data advantage.[379] Facebook's infrastructure and scale advantages are bound

---

[373] ibid.

[374] See inter alia 'The Cairncross Review - A Sustainable Future for Journalism'; Australian Competition & Consumer Commission (n 337).

[375] 'The Cairncross Review - A Sustainable Future for Journalism' (n 375) 14–15.

[376] ibid 17.

[377] ibid 22.

[378] 'Though platforms and news publishers acquire data on their users from the personal information that users willingly provide, people tend to enter much more personal data for a Facebook account, for instance, than for an account with a news publisher. This data, along with data about a user's browsing history (contained in a "cookie" in their internet browser), can be tailored for online advertising according to demographic, location, browsing and purchasing data […] Publishers will thus need to collect far more extensive information on their users, if they want to compete effectively for online advertising spend.' ibid 45.

[379] Access to large audiences and unparalleled volumes of data are identified as the main underlying causes of the Google/Facebook duopoly in online advertising. The Autorite de la Concurrence recently observed: '[the majority of publishers, advertisers and advertising service providers expressed […] that Google and Facebook form a duopoly in the online advertising sector that captures most advertising revenue and growth in the sector. Some feel that there will be less and less competition in the sector in the future. A significant number of players underlined the competitive advantage of having large audiences from the services provided to internet users. This enables Google and Facebook to sell adverting inventories and capitalise on huge volumes of data.' Autorité de la Concurrence (n 331) 36; The Cairncross Review arrived at similar conclusions: 'there is evidence to suggest that the two main online platforms – namely Google and Facebook – have significant market shares and influence over the advertising system, with a potentially detrimental effect on competition, including from publishers." "The Cairncross Review - A Sustainable Future for Journalism' (n 375) 60–61; Numbers lend support to these contentions. In Q1 2016 US online ad revenues 'hit a record-setting high at nearly $16 Billion'. However, it was estimated that 90% of the growth went to Google and Facebook. Jason Kint, 'Google and Facebook Devour the Ad and Data Pie. Scraps for Everyone Else.' (*Digital Content Next*, 16 June 2016)

to reduce the scope of competition even further. For example, Facebook has the ability to deliver ads on its own properties (mostly Facebook and Instagram, and indirectly on messaging functionalities if ads are sent by users) and on third-party publisher websites that are members of the Facebook Audience Network. The use of automatic placements on both inventories is likely to lower the overall cost of advertising campaigns,[380] for which reason advertisers are likely to be more inclined to choose Facebook's advertising services. Indeed, the *Cairncross Review* concluded that the position of Facebook in online display advertising, through its integrated infrastructure and 'vast repositories of data', is of such magnitude 'that challengers are effectively unable to enter the market', which may be indicative of 'grounds for intervention.'[381]

The improvement of Facebook's ad targeting capabilities, largely caused by its exploitative terms and deceptive behaviour, has made Facebook increasingly indispensable for advertisers, which is reflected in the exponential growth of its advertising revenues in recent years.[382] Facebook's annual advertising revenues went from USD 11.4 billion in 2014 to USD 55 billion in 2018.[383] As a result, advertisers have begun to suffer Facebook's market power on this side of the market.

For example, it has been argued that on some occasions the performance of Facebook's advertising services is overstated, which may be as a result of over reporting the number of visitors to its platform.[384] Similarly, it is claimed that the standards Facebook has adopted may mislead advertisers by overstating the number of consumers that have viewed their ads.[385] Indeed, Facebook has a rich history of miscalculating ad metrics.[386] For example, in 2017 ad videos served on Facebook mobile app continued to play after they were scrolled out of view, and Facebook charged advertisers for the background views.[387] Also, in 2016 Facebook admitted that it had been overstating the 'average duration of video viewed' metric.[388] Facebook reportedly told some advertisers that it had been 'probably' overstating the average time spent watching video ads by 60 per cent to 80 percent; however, a group of small advertisers claimed in a lawsuit that Facebook had instead inflated the average ad-watching time by 150 per cent to 900 per cent.[389] Importantly, complaints have been made that Facebook is measuring the performance of its own advertising services whilst restricting the ability of advertisers to resort to

<https://digitalcontentnext.org/blog/2016/06/16/google-and-facebook-devour-the-ad-and-data-pie-scraps-for-everyone-else/>.

[380] Autorité de la Concurrence (n 331) 55.

[381] 'The Cairncross Review - A Sustainable Future for Journalism' (n 375) 63.

[382] Bundeskartellamt (n 88) 4.

[383] See Forms 10-K "Annual Report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934" for the fiscal years ending on 31 December 2014 to 31 December 2018, filed by Facebook with the U.S. Securities and Exchange Commission, available at https://www.sec.gov/cgi-bin/browse-edgar?company=facebook&owner=exclude&action=getcompany

[384] Australian Competition & Consumer Commission (n 337) 77.

[385] ibid.

[386] For a list of measurement errors see Tim Peterson, 'FAQ: Everything Facebook Has Admitted about Its Measurement Errors' (*Marketing Land*, 17 May 2017) <https://marketingland.com/heres-itemized-list-facebooks-measurement-errors-date-200663>.

[387] ibid.

[388] Greg Finn, 'Facebook Acknowledges Discrepancy That Had Overstated a Video View Metric' (*Marketing Land*, 23 September 2016) <https://marketingland.com/facebook-acknowledges-discrepancy-overstated-video-view-metric-192828>.

[389] Ethan Baron, 'Facebook Lured Advertisers by Inflating Ad-Watch Times up to 900 Percent: Lawsuit' (*The Mercury News*, 16 October 2018) <https://www.mercurynews.com/2018/10/16/facebook-lured-advertisers-by-inflating-ad-watch-times-up-to-900-percent-lawsuit/>.

independent third parties to this end.[390] According to the *Australian Competition & Consumer Commission*, 'the inability for advertisers to verify the delivery and performance of their ads on […] Facebook has the potential to lessen competition in the supply of advertising services. This is because it has the potential to mislead advertisers into thinking their ads perform better than they actually do. This impedes the transmission of price and quality signals in the market and encourages some advertisers to advertise on [Facebook] rather than with competing suppliers of advertising services.'[391]

C. Prioritisation of traffic to derive a Competitive Advantage, to the detriment of news publishers

As seen above,[392] content publishers, especially news publishers, are Facebook's competitors, as they compete for users' time online, user data and advertising revenues. However, at some point in the early 2010s Facebook and news publishers decided to pause their competitive rivalry and reach a mutually beneficial deal. News publishers created Facebook pages and filled them with free high-quality content. This content increased the time users spent on the platform. In return Facebook provided news publishers traffic referrals, which significantly increased the visits to their websites.

At the beginning, news publishers were highly satisfied. Facebook's traffic referrals to news sites rose slowly and steady since at least 2012, and surpassed Google's referrals in 2015.[393] However, after news publishers had become fully dependent on Facebook's traffic, Facebook stopped fulfilling its side of the bargain. To keep users within the platform and therefore monopolise their attention and data, Facebook began to implement product changes that deterred users from leaving Facebook. Firstly, Facebook sent users to a built-in browser that loaded timeline links rather than sending the user to a full browser.[394] This meant that Facebook users who wanted to view content on publishers' websites outside Facebook could only use Facebook's in-app browser to this end. Notably, Facebook's built-in browser loaded on average three seconds slower than iOS's Safari.[395]

Since studies[396] show that users tend to abandon websites that take more than three seconds to load, Facebook's in-app browser had the effect of reducing the rate at which users click to content publishers' websites, and consequently the rate at which Facebook users share links to said websites. As a solution, Facebook offered news publishers 'the ability to publish content not on their own websites, but inside the walls of the impenetrable Facebook.'[397] With faster loading times, publishers' articles would be read. Indeed, Facebook marketed 'Instant Articles' as a solution to the mobile web-browsing problem of load times, and some publishers have reportedly indicated that the user

---

[390] Australian Competition & Consumer Commission (n 337) 77.
[391] ibid 79.
[392] See text accompanying footnote 372.
[393] Jillian D'Onfro, 'Facebook Is Now More Important than Google for Online Publishers' (*Business Insider*, 18 August 2015) <https://www.businessinsider.com/facebook-v-google-referral-traffic-2015-8>.
[394] Ryan Whitwam, 'The Facebook App Has Started Opening Web Links With A Built-In Browser For Some Users' (*Android Police*, 19 August 2014) <https://www.androidpolice.com/2014/08/19/the-facebook-app-has-started-opening-web-links-with-a-built-in-browser-for-some-users/>.
[395] The Capitol Forum, 'Facebook: The Capitol Forum Tested Facebook Browser Load Times; Facebook's Slow Load Times for In-App Browser Likely Push Users Towards Instant Articles and Native Content, Raising Antitrust Concern in EU'.
[396] 'How Loading Time Affects Your Bottom Line' (*Neil Patel*, 28 April 2011) <https://neilpatel.com/blog/loading-time/>.
[397] Srinivasan (n 138) 80–81.

experience through the in-app browser was poor enough to push them towards using Instant Articles.[398] Facebook has reported that users click on Instant Articles 20% more than other articles, and that they share Instant Articles 30% more than other web articles on average.[399]

For publishers, this was hardly a solution. Since Instant Articles are hosted on Facebook, publishers adopting this format ceased to get traffic to their sites. As a result, users' interactions with news publishers' websites decreased. In addition, publishers lost the ability to collect first-party audience data via cookies, and were forced to rely on the basic data provided by Facebook the accuracy of which is highly debatable.[400] Crucially, 'that data is the currency by which publishers build rich audience profiles to convince advertisers to run campaigns.'[401] Given the significance of consumer data to derive a competitive advantage and drive advertising revenues, the loss of data publishers suffered impaired their competitive performance. In addition, Facebook derived a new advertising revenue source. If a participating publisher sells an ad on its website, the publisher keeps 100% of the ad revenue; however, if Facebook sells the ad shown in an Instant Article on behalf of the publisher, Facebook keeps a 30% cut. [402]

Whilst Facebook denies[403] that its news feed algorithms prioritise Instant Articles through its ranking system, Instant Articles are organically prioritised and 'appear higher within News Feeds than non-Instant Articles content because their faster load times increase "interactions," such as clicks, likes, and comments.'[404] In addition, Facebook has made changes in its algorithms to give preference to native content, that is, content hosted on its platform, over non-native content such as content that refers users to publishers' websites. For example, a modification of Facebook's algorithms in 2015 was pointed our as the reason for significant drops in traffic for many of the world's biggest and best-known online news publishers, including the BBC, the Daily Mail, the New York Times, BuzzFeed and Fox News. These dips in traffic 'are highly worrisome to publishers who base their online advertising rates on the amount of traffic they receive.'[405] The algorithm change tried to 'ensure that content posted directly by the friends you care about, such as photos, videos, status updates or links, will be higher up in News Feed so you are less likely to miss it.'[406]

Then, in 2018, Facebook implemented a new change to its news feed algorithms to favour what Facebook called 'meaningful social interactions'.[407] The changes were aimed to favour interactions between friends and family, so the time users spend on Facebook would be

[398] The Capitol Forum (n 396) 4.
[399] Facebook, 'Facebook Instant Articles' <https://instantarticles.fb.com/>.
[400] See text accompanying footnotes 384to 390.
[401] The Capitol Forum (n 396) 5.
[402] Srinivasan (n 138) 81.
[403] Facebook, 'FAQ - Instant Articles - Documentation' (*Facebook for Developers*) <https://developers.facebook.com/docs/instant-articles/faq>.
[404] The Capitol Forum (n 396) 1.
[405] Lara O'Reilly, 'The Web Traffic for the World's Biggest Publishers Dropped Dramatically in April — and Nobody Can Agree Why' (*Business Insider*, 18 August 2015) <https://www.businessinsider.com/traffic-drops-for-daily-mail-buzzfeed-bbc-new-york-times-and-more-between-march-and-april-2015-8>.
[406] Facebook, 'Balancing Content from Friends and Pages | Facebook Newsroom' (21 April 2015) <https://newsroom.fb.com/news/2015/04/news-feed-fyi-balancing-content-from-friends-and-pages/>.
[407] Nicholas Thompson Vogelstein Fred, '15 Months of Fresh Hell Inside Facebook' [2019] *Wired* <https://www.wired.com/story/facebook-mark-zuckerberg-15-months-of-fresh-hell/>.

'time well spent'.[408] As a consequence, 'news content that is more directly consumed by users, if they don't talk about it or share it, [would] actually receive less distribution.'[409] Hence, the changes disfavoured stories published by media companies. Facebook promised that the effects of the change would be softened for news and publications that scored high on a user-driven metric of 'trustworthiness'.[410] However, it was subsequently discovered that the concept of 'trustworthy news' referred to stories involving 'politics, crime or tragedy.'[411] Accordingly, only inflammatory news, which are those that elicit more consumer engagement, would be to some extent exempted from the negative effects of the algorithm changes, to the detriment of any other news of any kind (such as health, since, technology or sports news). Some news publishers reported 40 to 50 percent drops in traffic to their websites after this algorithm change.[412]

This type of algorithmic design is one of the main reasons for the rise of fake news, widespread disinformation and political manipulation. Indeed, by '[b]y pulling technological levers that keep users on its platform, thereby lessening clicks to news publishers' sites, Facebook has sped the decline of legitimate news and provided a breeding ground for the fake variety.'[413] This is probably one of the reasons why Dow Jones CEO and WSJ publisher Will Lewis has accused Facebook of 'killing news.'[414]

However, this prioritisation of content has an anticompetitive dimension. Prioritising content that is either native to Facebook or that does not contemplate referrals to websites outside Facebook, in an effort to gain more traffic, data and market power, to the detriment of competitors, is remarkably similar to Google's abuse of dominance in the *Google Shopping* case. According to the Commission, Google engaged in a double practice consisting of systematically giving prominent placement to its own comparison shopping service, and demoting rival comparison shopping services in Google's search results. These practices resulted in a significant advantage compared to Google's rivals, in breach of EU antitrust rules.[415]

Similar to Google's conduct in those proceedings, Facebook lacks neutrality, prioritises content and features that benefit its platform, and discriminates competitors that that depend on traffic to compete on the merits, in contravention of Article 102(b) TFEU. The *Google Shopping* case showed that when a digital platform in a near-monopoly position competes with undertakings that depend on the platform for distribution, the prioritisation of the platform's interests to the detriment of competitors distorts the competitive process, harms innovation incentives, and warrants antitrust intervention.

---

[408] Fred Vogelstein, 'Facebook Tweaks Newsfeed to Favor Content from Friends, Family' [2018] *Wired* <https://www.wired.com/story/facebook-tweaks-newsfeed-to-favor-content-from-friends-family/>.
[409] ibid.
[410] Vogelstein (n 408).
[411] ibid.
[412] Australian Competition & Consumer Commission (n 337) 110.
[413] Sally Hubbard, 'Why Fake News Is An Antitrust Problem' (*Forbes*, 10 January 2017) <https://www.forbes.com/sites/washingtonbytes/2017/01/10/why-fake-news-is-an-antitrust-problem/>.
[414] Ian Burrell, 'Dow Jones Chief Accuses Google and Facebook of "Killing News"' (*The Drum*, 1 December 2016) <https://www.thedrum.com/opinion/2016/12/01/dow-jones-chief-accuses-google-and-facebook-killing-news>.
[415] European Commission, 'European Commission - PRESS RELEASES - Press Release - Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service' (2017) <http://europa.eu/rapid/press-release_IP-17-1784_en.htm>.

D. Foreclosure of Data to Exclude Competition

Facebook's social graph, that is, 'the information about one's relationships on [Facebook] that the user makes available to the system',[416] is one of Facebook's most valuable assets. Building a comprehensive network of connections normally involves a substantial period of time. Moreover, in this network, Facebook friends are not just names. Rather, they are specific individuals amongst many people often having the same name. Due to these reasons, recreating one's social graph manually is a highly laborious task.[417]

In spite of Facebook's claims to the contrary,[418] users cannot export their social graph onto other social networks or similar services. The Download Your Information tool that Facebook provides only renders a list of a user's friends' names and the dates on which the connections were made (i.e. when the friend request was confirmed), but it does not provide a unique username, a link to their Facebook profile or anything that may assist a user to find them on other services aside from manually typing their names. Therefore, Facebook has exclusive control over its users' social graphs.

To encourage app developers to write apps for Facebook, for years Facebook gave them access to its users' social graph through the Find Friends API, an IP-protected interface which effectively allows users to connect with their Facebook friends on other apps. This interoperability permission was essential to the viability and success of social apps. This is because social apps, just like Facebook, depend on connections between people, and only Facebook knows who people's real connections are. As tech journalist Josh Constine explains: 'if you want to jumpstart a social app, Facebook's Find Friends feature is very valuable. It can be the difference between an empty feed and low retention, and a vibrant, addictive feed teeming with content from people you care about.'[419]

However, after Facebook had gained unparalleled scale and attained a dominant position in the social network market, to protect that position, it began to deny apps it perceived as a competitive threat access to the Find Friends API, thereby impairing their growth potential.

For example, Voxer was a walkie-talkie mobile app that allowed users to talk to friends across iPhones and Android devices. In 2012 the app started to become viral, ranking in top places in the apps stores. It availed itself of the Find Friends API to propel adoption

---

[416] Roosendaal (n 130) 4.

[417] 'Reconfirming your social graph manually on other apps is awkward at worst and annoying at best. Think about it. If your Facebook account were reset and you had to send friend requests to all your old friends, how many do you think would confirm? Even your best friends might be too lazy to [...]' Josh Constine, 'Facebook Is Done Giving Its Precious Social Graph To Competitors' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/24/my-precious-social-graph/>; 'There are tons of John Smiths on Facebook, so finding him on another social network with just a name will require a lot of sleuthing, or guess-work. Depending on where you live, locating a particular Garcia, Smirnov or Lee could be quite difficult.' Josh Constine, 'Facebook Shouldn't Block You from Finding Friends on Competitors' (*TechCrunch*, 2018) <http://social.techcrunch.com/2018/04/13/free-the-social-graph/>.

[418] Question 30: Would Facebook support a requirement that users be allowed to download and take their data to competitive [sic] services? Facebook already allows users to download a copy of their information from Facebook. This functionality, which we've offered for many years, includes numerous categories of data, including About Me, Account Status History, Apps, Chat, Follower, Following, Friends, Messages, Networks, Notes, and more. Facebook, 'Post-Hearing Questions Pertaining to Hearing "Facebook, Social Media Privacy, and the Use and Abuse Data" Held on 10 April 2018 before the US Senate Committee on Commerce, Science and Transportation' 131.

[419] Constine, 'Facebook Is Done Giving Its Precious Social Graph To Competitors' (n 418).

and growth. Based on its growth potential it raised over USD 30 million in that year.[420] However, in 2013 Facebook copied Voxer by adding voice messaging to its Messenger app,[421] and two weeks later Facebook cut off Voxer's access to the Find Friends API.[422] Soon thereafter Facebook applied the same measure to Wonder,[423] a then-new social search app developed by the Russian search engine Yandex which combined its own proprietary search algorithms with social network data from Facebook, Twitter, Instagram and Foursquare, supporting searches on places, music and news.[424]

The same happened with Twitter's video app Vine.[425] Leaked internal Facebook documents[426] show that on the day Vine was launched in iOS's App Store Facebook executive Justin Osofsky wrote to Mark Zuckerberg: 'Twitter launched Vine today, which lets you shoot multiple short video segments to make one single, 6-second video. As part of their NUX, you can find friends via FB. Unless anyone raises objections, we will shut down their friends API access today. We've prepared reactive PR.' Mark Zuckerberg's response was 'Yup, go for it'.[427] The reactive PR took the form of a blog post by Osofsky, where he seemingly justified the decision to cut off Voxer, Wonder and Vine access to the Find Friends API based on alleged violations of Facebook's Platform Policy, which were 'further clarified' the day of the post.[428]

---

[420] Eric Eldon, 'Walkie Talkie App Voxer Goes Big, IVP And Intel Lead $30 Million Round' (*TechCrunch*, 2012) <http://social.techcrunch.com/2012/04/11/walkie-talkie-app-voxer-goes-big-ivp-and-intel-lead-30-million-round/>.

[421] Josh Constine, 'Facebook Adds Voice Messaging To Messenger For IOS and Android, Tests Open Source VoIP In Canada' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/03/facebook-voice-messaging/>.

[422] Josh Costine, 'Facebook Is Cutting Off Find Friends Data To "Competing" Apps That Don't Share Much Back, Starting With Voxer' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/18/facebook-data-voxer/>.

[423] Josh Costine, 'Facebook Blocks Yandex's New Social Search App From Accessing Its Data Just Three Hours After Launch' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/24/facebook-blocks-yandex-wonder/>.

[424] Ingrid Lunden, 'Yandex Confirms Wonder, A Voice-Powered Social Search App, As A U.S. "Experiment," Gets Legal Advice On Why It Shouldn't Irk Facebook' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/24/yandex-launches-social-search-app-wonder-as-a-u-s-experiment-gets-legal-advice-on-why-it-shouldnt-bother-facebook/>.

[425] Jeff Blagdon, 'Facebook Has Apparently Blocked Vine's Friend-Finding Feature' (*The Verge*, 24 January 2013) <https://www.theverge.com/2013/1/24/3913082/facebook-has-apparently-blocked-vines-friend-finding-feature>.

[426] The app developer Six4Three has been engaged in a legal battle with Facebook in California since 2015. Its founder, Ted Kramer, gained access through discovery to an array of Facebook internal documents which allegedly prove that Facebook had considered selling access to user data and had bypassed users' privacy preferences for its own commercial benefit, which ultimately enabled Cambridge Analytica to access and process data about 87 million people. Although the documents were being kept under seal in California, the Digital, Culture, Media and Sport Committee in the United Kingdom seized, and then made public, at least some of said documents whilst Ted Kramer was in London for business in November 2018. See Rebecca Hill, 'Facebook Spooked after MPs Seize Documents for Privacy Breach Probe' (26 November 2018) <https://www.theregister.co.uk/2018/11/26/facebook_dcms_document_cache_seized/>.

[427] Damian Collins, 'Note by Chair and Selected Documents Ordered From Six4Three' (November 2018) Exhibit 44 <https://www.documentcloud.org/documents/5433555-Note-by-Chair-and-Selected-Documents-Ordered.html>.

[428] Justin Osofsky, 'Clarifying Our Platform Policies' (*Facebook for Developers*, 25 January 2013) <https://developers.facebook.com/blog/post/2013/01/25/clarifying-our-platform-policies/>.

In particular, section I.10 of Facebook's then-in effect Platform Policy required apps using Facebook's data to allow users to share data back to Facebook, and prohibited the replication of a core Facebook functionality without permission.[429]

The problem with this explanation is that, at least Voxer and Vine *did* share data back to Facebook. Voxer had a 'share to Facebook' option,[430] and Vine users could share their short videos to the Facebook, Twitter and Vine feed from within the app.[431] Also, apps such as Viddy, YouTube Capture and iMovie all shared content to Facebook in the same manner as Vine did,[432] yet were not subject to the same restrictive measure. Moreover, Vine's main feature was the sharing of six-second looping videos (basically GIFs with sound), and Facebook's closest functionality at the time was standard video sharing on Facebook and photo sharing on Instagram.[433] Crucially, Voxer only replicated a core Facebook functionality after Facebook had copied Voxer's voice messaging feature. Accordingly, if Facebook decided to copy any functionality or app, the creator would be suddenly violating Facebook's policy.[434] The sequence of events could be also the other way around. For example, the app Phhhoto, which allowed users to shoot animated GIFs, was cut off from Instagram's social graph soon after reaching 1 million users, and six months later Instagram launched Boomerang, a blatant copy of Phhhoto.[435] As Constine observes: 'Facebook's selective enforcement of the policy is troubling. It simply ignores competing apps that never get popular. Yet if they start to grow into potential rivals, Facebook has swiftly enforced this policy and removed their Find Friends access, often inhibiting further growth and engagement.'[436] None of the apps mentioned above (the 'target apps') managed to remain on their respective markets for too long.

Facebook's sudden decision to cut off the target apps access to its Find Friends API is likely to constitute a refusal to supply interoperability information in contravention of Article 102(b) TFEU. It is settled case law that a dominant undertaking's refusal to licence a product protected by IP rights may be abusive only under special circumstances.[437] In particular, the refusal must relate to a product or service indispensable to the exercise of a specific activity on a neighbouring market; the refusal must exclude any effective

---

[429] The text read as follows: Reciprocity and Replicating core functionality: (a) Reciprocity: Facebook Platform enables developers to build personalized, social experiences via the Graph API and related APIs. If you use any Facebook APIs to build personalized or social experiences, you must also enable people to easily share their experiences back with people on Facebook. (b) Replicating core functionality: You may not use Facebook Platform to promote, or to export user data to, a product or service that replicates a core Facebook product or service without our permission. Costine, 'Facebook Clarifies Ban On Apps That Use Its Data To Replicate Its Features Or Don't Share Back' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/25/facebook-bans-replicating-its-functionality/> accessed 20 April 2019.

[430] Constine, 'Facebook Is Done Giving Its Precious Social Graph To Competitors' (n 418).

[431] Roberto Baldwin, 'Facebook Gets Passive-Aggressive About Blocking Vine' [2013] *Wired* <https://www.wired.com/2013/01/facebook-vine-policy/>.

[432] ibid.

[433] Costine, 'Facebook Clarifies Ban On Apps That Use Its Data To Replicate Its Features Or Don't Share Back' (n 430).

[434] For instance, after Snapchat declined Facebook's offer to acquire it, Facebook copied Snapchat and launched its own ephemeral messaging app named Poke. See Josh Constine, 'Facebook Launches Snapchat Competitor "Poke", An IOS App For Sending Expiring Text, Photos, And Videos' (*TechCrunch*, 2013) <http://social.techcrunch.com/2012/12/21/facebook-poke-app/> Suddenly, Snapchat was violating Facebook's no replication policy. .

[435] Constine, 'Facebook Shouldn't Block You from Finding Friends on Competitors' (n 418).

[436] ibid.

[437] *Joined Cases C-241/91 P and C-242/91 P, Radio Telefis Eireann (RTE) et Independent Television Publications (ITP) v Commission (Magill) [1995] ECR I-0743* para 50.

competition on said neighbouring market; the refusal must prevent the appearance of a new product for which there is potential consumer demand; and the refusal cannot be objectively justified.[438] However, these criteria have been to some extent relaxed by the General Court in high-tech markets exhibiting strong network effects, such as the markets involved in Facebook's refusal to supply under analysis.[439] In addition, the Commission has observed that there is no 'exhaustive checklist' of exceptional circumstances, and therefore 'other circumstances of exceptional character' may be taken into account to assess a refusal to supply,[440] so a refusal that does not fall squarely within the criteria above may still amount to an abuse.[441] For example, in *Commercial Solvents* and *Telemarketing* the disruption of previous levels of supply was relevant to the assessment of the refusal. In *Volvo,* the CJEU held that the exercise of an exclusive right by a dominant undertaking may infringe Article 102 TFEU if it entails 'certain abusive conduct such as the arbitrary refusal to supply spare parts to independent repairers, the fixing of prices for spare parts at an unfair level or a decision no longer to produce spare parts for a particular model even though many cars of that model are still in circulation.'[442] Accordingly, other important factors surrounding Facebook's conduct may be decisive to establish its abusive nature, and even if said conduct does not quite fit within the criteria above, it may nevertheless infringe Article 102 TFEU if it goes against the aim of preserving an effective competitive structure that benefits consumers.

It seems apparent that accessing the social graph of Facebook's users was indispensable for the activities of Voxer, Vine, Wonder and Phhhoto. Just like Facebook, social apps thrive on user engagement and traffic, for which reason they must be able in early stages to attract users to propel direct network effects and ultimately generate more data to train their algorithms and be able to offer a compelling service. Logically, users of these apps want to interact mainly with their friends and acquaintances, for which reason they are naturally drawn to apps where they can find them. Accordingly, access or lack of access to people's social graph is likely to dictate, in and of itself, the future success or failure of a new social app. If users cannot find their connections on a new social app, they will soon give up on it, especially given that they can find all of their connections on Facebook. In turn, low adoption of the app means that it will not be able to achieve critical mass, and therefore it will be bound to implode. Conversely, if users can find their connections on a new social app, it is likely that they engage with it, propel traffic and ultimately contribute to the app's improvement.

Crucially, there are no substitutes for the social graph of Facebook users. Given its dominant position in the social network market, only Facebook knows who people's real connections are. Reproducing one's social graph manually requires effort on the part of every user wanting to use a new social app, and as noted above, it is a cumbersome and ineffective exercise.[443] Also, Facebook users cannot export their social graphs onto other services. There may be other ways to reproduce users' real-life contacts, such as for example by accessing users' phonebook on their mobile devices to make contact

[438] *Case T-201/04, Microsoft Corp v Commission [2007] ECR II-3601* paras 332–333.
[439] *Case T-201/04, Microsoft Corp. v Commission [2007] ECR II-3601* (n 439).
[440] *COMP/C-3/37792 Microsoft [2004]* para 555.
[441] Indeed, before the GC in Microsoft the Commission contended that an 'automatic' application of the IMS Health criteria would have been problematic, and maintained that 'in order to determine whether such a refusal is abusive, it must take into consideration all the particular circumstances surrounding that refusal, which need not necessarily be the same as those identified in Magill and IMS Health.' *Case T-201/04, Microsoft Corp. v Commission [2007] ECR II-3601* (n 439) para 316.
[442] *Case 238/87, AB Volvo v Erik Veng [1988] ECR 6211* para 9.
[443] See text accompanying footnote 417.

suggestions on an app. However, alternative ways to reproduce people's social graphs like this one are unlikely to allow competing apps to become a 'viable' competitor and therefore be able to exercise effective competitive pressure on Facebook. This is proved by the tragic fate of the target apps. After a successful start, soon to be drastically halted by Facebook's practice under analysis, Voxer was forced to change its business model to business communications in less than 6 months, losing popularity and clearing the path for Facebook Messenger to thrive.[444] In turn, Phhhoto shut down within two years since it was denied access to Instagram's social graph, blaming Facebook for its demise.[445] Wonder was never able to operate properly, as its API calls were all blocked by Facebook only hours after its launch, and the core dataset it needed was provided via Facebook's API.[446] Vine managed to stay in the market for a couple of years, but it struggled to keep traction and Twitter ultimately shut it down by late 2016.[447] The fact that alternative ways to reproduce people's social graphs only allow for, at best, fringe competition on the part of competing social apps, reinforces the view that Facebook's Find Friends API is indispensable to them. As the General Court held with regard to the indispensability criterion in *Microsoft,* the 'question is whether the information [the disclosure of which is refused] is indispensable to any competitor seeking to carry on business on the relevant market as a viable competitive constraint and not as a *de minimis* player who has effectively left the market for a "niche" position.'[448]

Moreover, both Wonder and Phhhoto were forced out of their respective market segments as a result of Facebook's refusal, which fulfils the 'elimination of all competition' criterion laid down in *Magill*[449] and *Bronner*.[450] Furthermore, in *Microsoft* the General Court held that especially in markets characterised by strong network effects, where the elimination of competition is more difficult to revert,[451] it is not necessary to demonstrate that all competition on the downstream market is likely to be eliminated.[452] Rather, what is relevant 'for the purpose of establishing an infringement of Article [102 TFEU], is that the refusal at issue is liable to, or is likely to, eliminate all effective competition on the market',[453] and the fact that competitors of the dominant undertaking remain marginally active in market niches is insufficient to assert the existence of that competition.[454] Accordingly, Facebook's refusal to give Voxer and Vine access to its Find Friends API, both of which retained a marginal presence after said refusal before their demise, meets the 'elimination of all effective competition' criterion established in *Microsoft.* Crucially, Facebook's intent when effecting the refusal was precisely the elimination of competition from the target apps, an additional factor that reinforces the anticompetitive nature of Facebook's conduct. With the exception of Wonder, Facebook (and Instagram in the case of Phhhoto) had given access to the Find Friends API prior to the refusal, cutting off access only when it

[444] Constine, 'Facebook Shouldn't Block You from Finding Friends on Competitors' (n 418).
[445] Josh Constine, 'Phhhoto Shutters App and Pivots to Photobooths, Blaming Instagram' (*TechCrunch*, 2017) <http://social.techcrunch.com/2017/06/20/phhhoto-shuts-down/>.
[446] Ingrid Lunden, 'Wonder No More. Yandex Pulls Social Discovery App After Facebook Closes Door On Graph API Use + Says It's A Competing Search Engine' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/30/wonder-no-more-yandex-says-facebook-has-given-a-final-no-on-graph-api-usage-will-pull-its-social-app/>.
[447] Constine, 'Facebook Shouldn't Block You from Finding Friends on Competitors' (n 418).
[448] *Case T-201/04, Microsoft Corp. v Commission [2007] ECR II-3601* (n 439) para 355.
[449] *Joined Cases C-241/91 P and C-242/91 P, Radio Telefis Eireann (*RTE*) et Independent Television Publications (ITP) v Commission (Magill) [1995] ECR I-0743* (n 438) para 56.
[450] *Case C-7/97, Oscar Bronner GmbH & Co KG v Mediaprint [1998] ECR I-7791* para 41.
[451] *Case T-201/04, Microsoft Corp. v Commission [2007] ECR II-3601* (n 439) para 562.
[452] ibid para 563.
[453] ibid.
[454] ibid.

determined that the benefits it could derive from interoperability with the target apps were outweighed by the competitive threat their growing popularity could pose to Facebook. In the case of Wonder, Facebook decided to block its viability and potential growth from the start. Put in other words, Facebook disrupted previous levels of supply and otherwise denied access to an indispensable product as a preventive measure to hinder the growth of downstream and potential competitors that had the potential to reach a scale capable of exerting meaningful competitive pressure on it.

The question of whether Facebook's conduct under analysis meet the new product criterion may be also answered in the affirmative, based on a teleological interpretation of the same by reference to Article 102(b) TFEU. In *Magill*, the CJEU held that the refusal at hand was abusive because it prevented the appearance of a new product that was not offered by the dominant undertakings, and for which there was a potential consumer demand.[455] Facebook's refusal targeted at Wonder meets this criterion. Wonder was conceived to be an innovative voice-activated social search app. Users would be able to use their voices to enter searches such as 'restaurants in London my friends have visited', whereupon a scrolling interface would present the restaurants where their Facebook friends have taken photos or checked in.[456] Since Facebook blocked Wonder's access to its users' social graph only hours after being launched, Wonder could never make it into the marketplace. However, the refusals targeted at Voxer, Phhhoto and Vine did not prevent the appearance of a new product, as each of them had been launched and were operating before being cut-off access to Facebook and Instagram users' social graph. Yet, this fact in itself should not impede the characterisation of Facebook's conduct as abusive. Refusals to supply by dominant undertakings are prohibited under special circumstances because they contravene Article 102(b) TFEU that is, they limit production, markets and technical developments to the prejudice of consumers. Consequently, whether a refusal to licence an IP right prevents the appearance of a new product cannot be the only parameter which determines whether the refusal has ability to harm consumers within the meaning of Article 102(b) TFEU, given that consumers are also harmed when technical development is curtailed.[457]

Facebook's refusal prevented the target apps from developing and improving products that had great potential to scale and become viable alternatives to Facebook's social networking and messaging functionalities, thereby impairing consumer choice and technological progress. Importantly, since suddenly users of the target apps could not find their connections on them, due to the operation of direct network effects, they were naturally drawn back to the social network on which 'everybody is', as a result of which Facebook was able to both squash potential competitive threats and reinforce its dominant position in the social network market. Moreover, Facebook copied the functionalities that had elicited the original success of both Voxer and Phhhoto, thereby sending a powerful message to the market: Facebook gives access to its users' social graph only to apps the features of which do not overlap with any of Facebook's functionalities; however, if an app is growing strong based on new popular features, Facebook will cut off access to its API and replicate said features. As a consequence, Facebook discouraged app developers

[455] *Joined Cases C-241/91 P and C-242/91 P, Radio Telefis Eireann (RTE) et Independent Television Publications (ITP) v Commission (Magill) [1995] ECR I-0743* (n 438) para 54.
[456] Josh Constine, 'Russian Giant Yandex Has Secretly Built A Killer Facebook Search Engine App Codenamed "Wonder"' (*TechCrunch*, 2013) <http://social.techcrunch.com/2013/01/11/yandex-wonder/>.
[457] *Case T-201/04, Microsoft Corp. v Commission [2007] ECR II-3601* (n 439) para 647.

from developing and marketing new innovative social apps,[458] to the detriment of consumers, given that Facebook could at any time deny them access to the most significant driver of user engagement, copy their innovations and leverage its user base to ensure the success of its copycat functionalities.[459] Therefore, although Facebook's refusal targeted at Voxer, Phhhoto and Vine did not prevent the appearance of new products, it nevertheless impaired technical development and chilled app developers' innovation incentives, to the prejudice of consumers, for which reason the criterion relating to the appearance of a new product, as interpreted in *Microsoft*, is likely to be met.

It is unlikely that Facebook could be able to justify its refusal based on an objective justification. In the light of *Microsoft*, the fact that mandated access to an IP right may eliminate future incentives to create more intellectual property and engage in more innovation is not a valid objective justification for the refusal,[460] not least where such conduct eliminates the dominant undertaking's competitors' innovation incentives. Moreover, Facebook continued giving access to its API to apps that it did not considered as a competitive threat,[461] for which reason a reduction in innovation incentives as a result of mandated access to its Find Friends API would be a particularly unconvincing defence.

Facebook could claim that its refusal to give access to its API and the underlying data was motivated by privacy and security considerations. Needless to say, Facebook has a lot of work to do to protect the privacy of its users. Removing 'overly permissive APIs, even at the cost of some amount of competition and interoperability, can be necessary for that purpose – as with the Cambridge Analytica incident.'[462] However, privacy and security must not be used as an excuse to conceal anticompetitive elimination of actual and potential competitors. When a dominant platform removes an existing API or limits the data and/or functionality made available or enabled by the API, such decision may lead to a substantial reduction in consumer welfare that may outweigh the improvements in privacy and security that allegedly motivated that decision. Given Facebook's longstanding record of blatant disregard for its users' privacy,[463] an objective justification for its refusal based on privacy protection and security considerations should be seen with the utmost suspicion.

Facebook has already invoked privacy considerations to restrict interoperability and promote its own interests, harming the viability of thousands of apps that relied on its data at the same time. In 2014 Facebook removed the extended permissions from the Graph API v1.0, allegedly based on its users' preferences for 'private communication'[464] and the

---

[458] See Symons and Bass observing how powerful platforms can harm innovation: "At present, some platforms do make their data available through APIs in their websites. For instance, Facebook allow developers to build on top of their platform with access to data […] However, companies will set the rules about the sharing of their own data. Facebook use their API to control who gets access to customers' social graph, Facebook Connect and Graph API. They can use this to cut off any developer who poses a competitive threat. The result is that few developers invest seriously in creating alternatives." Tom Symons and Theo Bass, 'Me, My Data and I: The Future of the Personal Data Economy - A Report for the European Commission' (2017) 27–28.

[459] See text accompanying footnote 496.

[460] *Case T-201/04, Microsoft Corp. v Commission [2007] ECR II-3601* (n 439) paras 688–702.

[461] See text accompanying footnote 432.

[462] Chris Riley, 'Meet the Newest Walled Garden' (*Mozzila Blog - Open Policy & Advocacy*, 11 March 2019) <https://blog.mozilla.org/netpolicy/2019/03/11/meet-the-newest-walled-garden>.

[463] See Section II.C.

[464] In an interview with the New York Times in 2014 Zuckerberg said: 'Private communication has always been an important part of the picture, and I think it's increasingly important […] Anything we can do that makes people feel more comfortable is really good.' Vindu Goel, 'Some Privacy, Please? Facebook, Under

need to increase user trust.[465] Without these permissions, and particularly, without the data an app could access based on said permissions, many apps could not operate. An example was the app called Pikinis, which sought to collect pictures of women in bikini and show them in an organised manner. The app required access to users' friend list in order to go through that list and detect pictures featuring women in bikini. Another example was the app 'Pink Ribbon', designed to raise breast cancer awareness. The app required access to the 'full friends list API and other Graph API endpoints' to reach the largest amount of users possible to convey its message.[466]

Whilst the removal of extended permissions was a good measure to improve Facebook users' privacy, leaked internal documents show that Facebook did so as leverage over apps in a move to gain another revenue stream and improve its market position.[467] The documents show that Facebook considered several ways to charge third party apps for access to Facebook users' data, including direct payment, advertising spending and data-sharing arrangements.[468] Privacy considerations are largely absent in the documents, and when present, are only mentioned in the context of how could Facebook use privacy as a public relations strategy to contain the backlash following the changes to developers' access to users' data. Ultimately, Facebook decided not to sell its users' data directly, but instead to provide it to app developers that were considered 'special partners' or which would spend money on Facebook and share back their data to Facebook.[469] Indeed, '[t]he idea of linking access to friends data to the financial value of the developers relationship with Facebook is a recurring feature of the documents.'[470] This is reflected in some of the Facebook internal communications included in the leaked documents. For example, an executive of Badoo (a dating app) wrote to Konstantinos Papamiltidas, Director of Platform Partnerships at Facebook: 'we have been compelled to write to you to explain the hugely detrimental effect that removing friend permissions will cause to our hugely popular (and profitable) applications Badoo and Hot or Not. The friends data we receive from users is integral to our product (and indeed a key reason for building Facebook verification into our apps).'[471] In response, in a thread of emails from Papamiltidas it is discussed and confirmed that the apps had been 'whitelisted' (i.e. given preferential access

---

Pressure, Gets the Message' *The New York Times* (20 December 2017) <https://www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html>.

[465] See Mark Zuckerberg in the 2014 f8 conference: 'Over the years, one of the things we've heard over and over again is that people want more control over how they share their information, especially with apps, and they want more say and control over how apps use their data […] And we take this really seriously because if people don't have the tools they need to feel comfortable using your apps, that's bad for them and that's bad for you." https://www.youtube.com/watch?v=DVu311G5qvI

[466] Cyrus Farivar, 'Bikini App Maker Draws Another Disgruntled Developer to Its Facebook Fight' (*Ars Technica*, 7 December 2018) <https://arstechnica.com/tech-policy/2018/12/facebook-weaponized-user-data-app-developers-new-lawsuit-claims/>.

[467] The documents were leaked to journalist Duncan Campbell, who in turn shared them with a number of media organisations such as NBC News and Computer Weekly. About 400 of the 4,000 pages had been already made available by the Digital, Culture, Media and Sport Committee in the United Kingdom, which was investigating Facebook's data privacy practices following the Cambridge Analytica scandal. Olivia Solon and Cyrus Farivar, 'Thousands of Leaked Facebook Documents Show Mark Zuckerberg as "Master of Leverage" in Plan to Trade User Data' (*NBC News*, 16 April 2019) <https://www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706>.

[468] ibid.

[469] ibid.

[470] Collins (n 428) 1.

[471] ibid 130–131.

to users' data).[472] Similar emails leading to the same outcome were exchanged between Facebook and Lyft,[473] AirBnB[474] and Netflix.[475] Importantly, the documents also show that cutting off data access to certain apps was a conscious decision to impair their growth and protect Facebook's position.[476]

In short, Facebook has claimed that privacy concerns have been its main motivation to effect interoperability restrictions, in circumstances where the changes were actually driven by an intent to extract money from app developers, using its users' data as a bargaining chip. Facebook has demonstrated over and over again that its statements cannot be trusted. This is why competition authorities should be particularly wary of important changes implemented by Facebook that are capable of impairing the competitive performance of actual and potential competitors, especially when they are allegedly driven by privacy and security concerns, be it in the context of a potential abuse of dominance, a merger or in other scenarios. For example, Mark Zuckerberg recently posted a detailed explanation of his 'Privacy-Focused Vision for Social Networking', under which WhatsApp, Messenger and Instagram would be integrated into one privacy and security-oriented platform driven by principles such as 'private interactions', 'safety' and 'interoperability'. [477] Is this something people should believe? It is safe to answer in the negative. This vision is more likely to be an effort to consolidate Facebook's 'walled garden', where people can only communicate and interact with their connections using Facebook's products and features, but not those of competing services. As Riley observes, '[r]ather than creating the next digital platform to take the entire internet economy forward, encouraging downstream innovation, investment, and growth, Facebook is closing out its competitors and citing privacy and security considerations as its rationale.'[478]

E. Use of a Spyware App to Make Strategic Decisions and Distort Competition

In 2013 Facebook acquired the mobile-analytics company Onavo,[479] creator of the Onavo Protect app, which offered a number of security features including security alerts and access to a virtual private network (VPN) service. VPNs create a virtual encrypted tunnel between users and a remote server operated by a VPN service. All external Internet traffic

[472] 'We have now whitelisted Badoo [...] Hotornot [...] and Bumble [...] for the Hashed Friends API that was shipped late last night.' ibid 128.
[473] ibid Exhibit 87.
[474] ibid Exhibit 91.
[475] ibid Exhibit 92.
[476] 'In a March 2013 discussion, Justin Osofsky, then director of platform partnerships, described restricting the MessageMe app from accessing Facebook data because it had grown too popular and could compete with Facebook messages. He asked colleagues to see if any other messenger apps have "hit the growth team's radar recently." […] "If so, we'd like to restrict them at the same time to group this into one press cycle," he wrote in an email.' See also an extract from a December 2013 chatlog between several senior engineers talking about the removal of the extended permissions: 'Bryan Klimt: "So we are literally going to group apps into buckets based on how scared we are of them and give them different APIs? ... So the message is, 'if you're going to compete with us at all, make sure you don't integrate with us at all'? I'm just dumbfounded." Kevin Lacker: "Yeah this is complicated." David Poll: "More than complicated, it's sort of unethical."' Solon and Farivar (n 468).
[477] Mark Zuckerberg, 'A Privacy-Focused Vision for Social Networking | Facebook' (6 March 2019) <https://m.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/?notif_id=1551899118427378&notif_t=notify_me>.
[478] Riley (n 463).
[479] Reed Albergotti, 'Facebook Acquires Onavo, Gaining Office in Israel' (*WSJ*, 14 October 2013) <https://blogs.wsj.com/digits/2013/10/14/facebook-deal-gives-it-office-in-israel/> accessed 15 March 2019.

is channelled through this tunnel, and a user's computer appears to have the IP address of the VPN service. This allows users to secure their personal information by establishing secure connections when using public wi-fi hotspots or while working remotely. It also allows users to hide their location, identity and Internet activities from their Internet service provider and to bypass geographic restrictions on websites. Privacy policies of leading VPN providers, such as Private Internet Access, NordVPN and TorGuard are consistent with this objective and explicitly state that they do not log online traffic when consumers use their VPN services.[480]

For years Facebook provided Onavo Protect as a typical VPN to consumers, advertising it as an app that helps users to protect their mobile data and personal information.[481] However, according to Onavo's privacy policy, Facebook can receive all of a user's mobile data traffic, including location data and information about users' apps usage. In particular, after a user downloads and agrees to use the Onavo app, the user's mobile data traffic is sent through or to Facebook's server, which consequently receives personally identifying information such as the user's name, email address, or other contact information. Also, Facebook can use the information it receives to operate and improve its services, develop new products and services, analyse usage of Facebook's apps and other applications on the user's device, support advertising and related activities, and for other purposes.[482]

Accordingly, Facebook portrayed Onavo as a means for users to block malicious websites, keep their traffic safe and protect their data privacy, whilst Facebook itself was accessing and analysing that traffic. The insights Facebook derived from analysing mobile traffic enabled it to identify new trends in the mobile ecosystem. For example, Facebook would get an early heads up about apps that were becoming breakout hits; it could also tell which apps were seeing slowing user growth; and it could see which apps' new features were becoming popular.[483] Knowledge of these trends, in turn, was the driver of some important strategic decisions and acquisitions by Facebook. According to the note accompanying Facebook's internal documents recently released by UK MP Damian Collins, 'Facebook used Onavo to conduct global surveys of the usage of mobile apps by customers, and apparently without their knowledge. They used this data to assess not just how many people had downloaded apps, but how often they used them. This knowledge helped them to decide which companies to acquire, and which to treat as a threat.'[484]

Internal Facebook documents show that Facebook spent months tracking WhatsApp based on Onavo data, as a result of which Facebook realised about WhatsApp's impressive growth and usage trends. Facebook used data collected by Onavo to build 'industry update' presentations that informed on the reach of several social media and messaging apps, as

---

[480] See 'Private Internet Access Anonymous VPN' <https://www.privateinternetaccess.com/pages/privacy-policy/>; 'Privacy Policy' (*NordVPN*, 7 June 2016) <https://nordvpn.com/privacy-policy/>; 'Privacy Policy' (*TorGuard*) <https://torguard.net/privacy.php>.

[481] According to the Onavo website, 'Onavo Protect for Android helps you take charge of how you use mobile data and protect your personal info. Get smart notifications when your apps use lots of data and secure your personal details', and 'Onavo Protect for iPhone and iPad helps keep you and your data safe when you go online, by blocking potentially harmful websites and securing your personal information.' Onavo, 'Onavo | Home' <https://www.onavo.com/>.

[482] Onavo, 'Onavo | Privacy Policy' <https://www.onavo.com/privacy_policy>.

[483] Sarah Perez, 'Facebook Is Pushing Its Data-Tracking Onavo VPN within Its Main Mobile App' (*TechCrunch*, March 2018) <http://social.techcrunch.com/2018/02/12/facebook-starts-pushing-its-data-tracking-onavo-vpn-within-its-main-mobile-app/>.

[484] Collins (n 428) 1.

well as their evolution. In particular, Onavo's US mobile app charts for iPhone showed that WhatsApp was progressively gaining market reach, surpassing apps such as Tumblr, Foursquare, Vine and Google+.[485] Similarly, Onavo data from April 2013 showed that WhatsApp was sending 8.2 billion messages per day, largely surpassing Facebook Messenger's 3.5 billion.[486] Onavo data also showed that WhatsApp was outpacing Facebook Messenger in engagement time. A few months after Facebook's acquisition of Onavo, Facebook acquired WhatsApp.

It has also been reported that Onavo helped shaped Facebook's live-video strategy. Facebook's employees could see usage patterns for live-video apps like Meerkat and Twitter's Periscope. Based on this knowledge, Facebook made the decision to add a live-video feature to the Facebook app in 2016.[487] Similarly, Houseparty, an app that let groups of people hang out over video on smartphones, was quickly gaining popularity in 2016. Soon thereafter, Facebook executives approached Houseparty for meetings, to explore an acquisition. Then, two months after Houseparty advertised itself as 'the Internet's living room', Facebook's Messenger informed that it would become a 'virtual living room.'[488] Based on Onavo data, Facebook had spotted Houseparty's explosive growth.[489] After Facebook executives informed Houseparty that the conversations had not progressed, Facebook introduced a feature to the Messenger app which allowed users to see up to six people in a conversation, as compared to the eight-person rooms supported by Houseparty.[490] Ultimately, Facebook ended up launching its own live group-chat app, Bonfire, a clone of Houseparty.[491]

In a similar vein, internal presentations based on Onavo data depicted Snapchat as a potential threat as of April 2013.[492] Whilst Facebook and Instagram led in US mobile apps for iPhone, Snapchat was nevertheless growing fast, reaching a 13.2 per cent market share and ranking 16. Conversely, Facebook's Messenger had a 13.7 per cent market share, and ranked 15. Onavo data reportedly revealed to Facebook how many Snaps were sent every day on Snapchat.[493] That year Facebook attempted to acquire Snapchat for USD 3 billion, but Snapchat's CEO rejected the offer.[494] After the failed acquisition attempt, Facebook decided to devote its efforts to copy the features that led to Snapchat's initial success, including Stories (i.e. a public feed of photos and videos that disappear after 24 hours) and augmented reality features.[495] Facebook initially introduced its own version of Stories on

---

[485] ibid 12.
[486] ibid 14.
[487] Deepa Seetharaman and Betsy Morris, 'Facebook's Onavo Gives Social-Media Firm Inside Peek at Rivals' Users' *Wall Street Journal* (13 August 2017) <https://www.wsj.com/articles/facebooks-onavo-gives-social-media-firm-inside-peek-at-rivals-users-1502622003>.
[488] Betsy Morris and Deepa Seetharaman, 'The New Copycats: How Facebook Squashes Competition From Startups' *Wall Street Journal* (9 August 2017) <https://www.wsj.com/articles/the-new-copycats-how-facebook-squashes-competition-from-startups-1502293444>.
[489] ibid.
[490] ibid.
[491] Aatif Sulleyman, 'Facebook's New App Wants to Change How You Chat to Friends Online' (*The Independent*, 14 September 2017) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-bonfire-video-chat-app-friends-develop-feature-social-media-network-a7946261.html>.
[492] Collins (n 428) 12.
[493] Seetharaman and Morris (n 488).
[494] Scott Thurm, 'Snapchat Spurned $3 Billion Acquisition Offer from Facebook' (*WSJ*, 13 November 2013) <https://blogs.wsj.com/digits/2013/11/13/snapchat-spurned-3-billion-acquisition-offer-from-facebook/> accessed 30 April 2019.
[495] Karissa Bell, 'While You Weren't Looking, Facebook Hit Snap Where It Hurts Most' (*Mashable*, 3 May 2018) <https://mashable.com/2018/05/02/facebook-stories-crushing-snapchat/>.

Instagram, thereby leveraging its then-user base comprised of 500 million users. Stories on Instagram elicited more traffic and user engagement, and at the same time removed the motivation for Instagram's users to give a try to Snapchat.[496] Instagram's Stories quickly surpassed Snapchat's[497] and directly kneecapped Snapchat, the growth of which was slowed by 82 per cent at the end of 2016.[498] Facebook subsequently rolled out Stories on Facebook, Messenger and WhatsApp, and according to Facebook's Chief Product Officer Chris Cox, '[t]he Stories format is on a path to surpass feeds as the primary way people share stuff with their friends sometime [in 2019].'[499] Snapchat has not recovered from the effect of Facebook's copycat versions of its original feature. According to Snap's 2018 Q4 earnings report, Snapchat's daily active users shrank from 187 million in Q4 2017 to 186 million in Q4 2018.[500] Therefore, not only is Facebook growing the number of its Stories users; Snapchat is actually losing them.

Facebook has defended the use of the Onavo app by noting that 'websites and apps have used market research services for years.'[501] In addition, Facebook can readily defend its acquisition of WhatsApp by pointing out that it was approved by both the FTC and the Commission. Moreover, copyright law protects the expression of an idea rather than the idea itself, for which reason copying software features (i.e. an idea) is not a copyright infringement as long as the expression of the copied feature is different. Therefore, Facebook can argue that its strategy to mimic the successful functionalities of competitors is fair game. However, the EU Courts have repeatedly stressed the 'special responsibility of dominant undertakings not to allow their conduct to impair genuine undistorted competition',[502] as well as the prohibition imposed on dominant firms from eliminating competition by 'utilising methods other than those which come within the scope of competition on the merits.'[503] Since Facebook's pattern of behaviour described in this section is manifestly inconsistent with that special responsibility, falls outside the scope of competition on the merits and has the ability to cause actual and potential anticompetitive effects, an argument can be made that such behaviour by Facebook amounts to an abuse of a dominant position contrary to Article 102(b) TFEU.

The CJEU has held that '[c]ompetition on the merits may, by definition, lead to the departure from the market or the marginalisation of competitors that are less efficient and so less attractive to consumers from the point of view of, among other things, price, choice, quality or innovation.'[504] Coupled with dominant firms' 'special responsibility', this means that dominant undertakings are allowed to protect and reinforce their market position only by offering products and services at lower prices, of greater quality, or by increasing choice and/or their innovative activity to the benefit of consumers. Facebook's

---

[496] Ben Thompson, 'The Audacity of Copying Well' (*Stratechery by Ben Thompson*, 3 August 2016) <https://stratechery.com/2016/the-audacity-of-copying-well/>.
[497] Cara McGoogan, 'Instagram Stories Overtakes Snapchat with 200m Daily Users' *The Telegraph* (13 April 2017) <https://www.telegraph.co.uk/technology/2017/04/13/instagram-stories-overtakes-snapchat-200m-daily-users/>.
[498] Josh Constine, 'Snapchat Growth Slowed 82% after Instagram Stories Launched' (*TechCrunch*, 2016) <http://social.techcrunch.com/2017/02/02/slowchat/>.
[499] Bell (n 496).
[500] https://investor.snap.com/~/media/Files/S/Snap-IR/press-release/q4-18-earnings-release.pdf
[501] Facebook, 'Post-Hearing Questions Pertaining to Hearing "Facebook, Social Media Privacy, and the Use and Abuse Data" Held on 10 April 2018 before the US Senate Committee on Commerce, Science and Transportation' (n 419) 123.
[502] *Case 322/81, Nederlandsche Banden Industrie Michelin v Commission (Michelin I) [1983] ECR 3461* para 70.
[503] *Case C-457/10 P, AstraZeneca v Commission [2012] ECLI:EU:C:2012:770* (n 312) para 75.
[504] *Case C-209/10, Post Danmark A/S v Konkurrenceradet (Post Danmark I) [2012] ECR I-0000* (n 318) para 22.

use of Onavo, conversely, amounts to anticompetitive 'nowcasting'[505] that distorts the competitive process to the prejudice of consumers. By using its privileged access to mobile usage data, Facebook has been able to monitor new business models in real time and quickly identify and squash emerging competitive threats. Based on its privileged information, Facebook has acquired and attempted to acquire startups before they were able to exert meaningful competitive pressure on Facebook, and well before such starups became visible to competition authorities. And when the acquisition route has not worked, Facebook has copied the innovations of the startups it has sought to absorb and/or squelch. As a consequence, Facebook has significantly reduced startups' incentives to compete and innovate, reinforcing its position at the same time. Facebook's conduct is all the more reproachable given that it availed itself of consumers' known lack of engagement with and poor understanding of privacy policies to lure them to download Onavo for security purposes, whilst in practice Onavo enabled Facebook to analyse its users' activities on their mobile devices with remarkable detail.

The advantage Onavo gave Facebook beggars belief, making visible trends and likely futures which not even competition authorities could see. Take the example of the *Facebook/WhatsApp* merger.[506] The Commission found that Facebook was active in the market for consumer communications apps, social networking services and online advertising services, and that Facebook collects data about the users of its social network and analyses them in order to serve advertisements that are as much as possible 'targeted' at each particular user.[507] On the other hand, the Commission found that WhatsApp was active in the market for consumer communications services, and that WhatsApp did not sell any form of advertising and did not collect or store data about its users that would be valuable for advertising purposes.[508] The Commission also found that Facebook and WhatsApp competed with each other only in the market for consumer communications apps; however, its offerings were 'different in several respects', for which reason they were not close competitors.[509]

One of the theories of harm analysed by the Commission was that the merged entity could start collecting data from WhatsApp users with the aim of improving the accuracy of the targeted ads served on Facebook's social networking platform to WhatsApp users that are also Facebook users.[510] However, it was suggested in the proceedings that the merged entity would not have the incentive to start collecting data from WhatsApp users, as this data collection could prompt some users to switch to other consumer communications apps that they could perceive as less intrusive.[511] Moreover, the Commission analysed a potential concentration of Facebook's and WhatsApp's data only to the extent that it was likely to strengthen Facebook's position in the online advertising market or any sub-segments thereof,[512] and held that even if the merged entity started using WhatsApp user data to improve targeted advertising, competition concerns were unlikely to arise, as there would still remain large volumes of user data that are valuable for advertising purposes and that are not within Facebook's exclusive control.[513]

---

[505] Maurice E Stucke, 'Should We Be Concerned About Data-Opolies?' (2018) 2 Georgetown Law Technology Review 275, 305.
[506] *Case COMP/M.7217, Facebook/WhatsApp (2014)* (n 15).
[507] ibid para 70.
[508] ibid para 71.
[509] ibid paras 101, 107.
[510] ibid para 180.
[511] ibid para 186.
[512] ibid para 164, 187.
[513] ibid para 189.

The Commission's merger assessment is problematic, because it is extremely static with excessive reliance on narrowly defined markets. This approach sits at odds with the reality of dynamic markets where the pace of development blurs the distinction between different software functionalities, oftentimes resulting in new highly-integrated products composed of many features that once were offered on a stand-alone basis.[514] Also, the assessment is too simplistic, because it did not consider the myriad ways in data-driven externalities could reinforce Facebook's position not only in the display advertising market,[515] but also in the social network market.[516] But the important point to note here is that the Commission, in spite of its vast experience in assessing concentrations in the high-tech sector, *did not* perceive WhatsApp as entity likely to evolve into a market player capable of disciplining and even challenging Facebook or other dominant data-driven platforms, [517] whilst Facebook, based on its knowledge of WhatsApp's explosive growth, reach, and usage metrics, *had the certainty* that WhatsApp was going to become a competitive threat in the near future. Whilst the Commission saw WhatsApp as an unprofitable start-up with a large user base in a fragmented market, which would have otherwise gone under its radar had it not been for Facebook's proposed acquisition, Facebook had the tools and information to determine that WhatsApp was a potential future 'Facebook killer'.

Indeed, there is a very good example, albeit little-known in the West, of a messaging app that evolved into an ecosystem in its own right: Tencent's WeChat. It was launched in 2011 as a mobile-only messaging app with basic features such as text messaging, voice clips and photo sending. However, over time it added myriad functionalities that fuelled its success and popularity. In its current version, along with its basic communication features, WeChat users in China can access services to hail a taxi, order food delivery, buy movie tickets, play casual games, check in for a flight, send money to friends, access fitness tracker data, book a doctor appointment, get banking statements, pay the water bill, find geo-targeted coupons, recognise music, search for a book at the local library, meet strangers around you, follow celebrity news, read magazine articles, and even donate to charity.[518] Given WhatsApp's large user base and growing popularity prior to its acquisition by Facebook, it is not far-fetched to imagine that WhatsApp could have evolved into something similar or an otherwise powerful competitive force. However, Facebook's anticompetitive nowcasting radar system prevented this alternative, yet plausible future.

---

[514] For example, a Smartphone is composed of a camera, calculator, email interface and many other features that once were independent products.

[515] The analysis of metadata, that is, the vast amount of context surrounding a message that can be viewed even when the content is encrypted, could be used to improve ad targeting. According to encryption expert Alan Woodward, '[b]y abstracting out and looking at who's talking to who, for how long, and when . . . you can build up a very statistical picture of people very quickly […] In many ways, it is the context of what you say in those messages that is more important than the messages themselves.' Hannah Murphy, 'How Facebook Could Target Ads in Age of Encryption' (*Financial Times*, 27 March 2019) <https://www.ft.com/content/0181666a-4ad6-11e9-bbc9-6917dce3dc62>.

[516] Since August 2016 the phone numbers of WhatsApp users began to be shared with Facebook, which enabled the latter to run analytics on user activity and make friends suggestions based on people with whom users talk on WhatsApp. Michael Duran, 'How to Stop WhatsApp From Giving Facebook Your Phone Number' [2016] *Wired* <https://www.wired.com/2016/08/how-to-stop-whatsapp-from-sharing-your-phone-number-with-facebook/> In turn, more friends connections translate into more user engagement and therefore more data to train its social network algorithms and enhance further its ad targeting capabilities.

[517] Indeed, Google seems to have been aware of the threat posed by WhatsApp, as it also attempted to buy it. See Tom Warren, 'Google Reportedly Offered $10 Billion for WhatsApp' (*The Verge*, 20 February 2014) <https://www.theverge.com/2014/2/20/5429236/google-reportedly-offered-10-billion-for-whatsapp>.

[518] Connie Chan, 'When One App Rules Them All: The Case of WeChat and Mobile in China' (*Andreessen Horowitz*, 6 August 2015) <https://a16z.com/2015/08/06/wechat-china-mobile-first/>.

Facebook's efforts to eliminate nascent competitive threats did not stop when the acquisition route did not succeed. As seen with the examples of Houseparty[519] and Snapchat[520] above, Facebook is not ashamed[521] to copy the innovations that triggered the early adoption of the start-ups that it sees as a potential acquisition target, a strategy that has proved remarkably effective in impairing their competitive performance and growth.[522] That is due to the power and gravity of Facebook's and Instagram's user base. Facebook and Instagram users have no incentive to download a new app with attractive features if they can use the same features on the app where all their connections are. It is remarkable how history repeats itself, albeit with (slightly) different players. Microsoft tried to buy the nascent browser company Netscape in the 90s.[523] When that acquisition attempt failed, Microsoft included several features of Netscape's browser into its own browser, and made it freely available to consumers. Ultimately, Microsoft's attacks against Netscape got it in big trouble.[524]

Critics of antitrust enforcement in high-tech sector commonly rely on Schumpeter's 'dynamic competition[525] conception to advance their hands-off approach agenda. In dynamically competitive markets, the competitive race does not reward the producer selling more at the lowest price, but rather the innovator who comes up with the best 'killer' product that conquers the entirety of the market. Schumpeter also noted that this process of 'creative destruction' is the main source of economic progress and growth[526], for which reason, if the promotion of consumer welfare lies at the core of competition policy, it should foster dynamic competition instead of its 'weaker cousin', static competition.[527] Crucially, 'competition in high technology markets is frequently characterized by incremental innovation, punctuated by major paradigm shifts. These shifts frequently cause incumbents positions to be completely overturned… [for which reason] antitrust authorities need to be cognizant of the self-correcting nature of any dominance that is obtained in a particular regime [… as] market dominance in technologically progressive industries is likely to be transitory.'[528]

However, this competition dynamic above requires that markets remain open and innovative activity be not impaired and discouraged. Facebook's conduct described in this section achieves exactly the opposite, since it prevents the potential emergence of any

[519] See text accompanying footnote 491.
[520] See text accompanying footnote 495.
[521] The Wall Street Journal has reported that Mark Zuckerberg told Facebook employees at a meeting that they shouldn't let pride get in the way of serving users, which was another way of saying they shouldn't be afraid to copy rivals, according to someone who was at the meeting. The message became an informal internal slogan: "Don't be too proud to copy." Morris and Seetharaman (n 489).
[522] See text accompanying footnote 500.
[523] Matt Rosoff, 'Worst Miss Ever? Microsoft Tried To Buy Netscape In 1994' (*Business Insider*, 28 October 2011) <https://www.businessinsider.com/worst-miss-ever-microsoft-tried-to-buy-netscape-in-1994-2011-10>.
[524] *United States v. Microsoft Corporation*, 253 F.3d 34 (D.C. Cir. 2001),
[525] Joseph A Schumpeter, *Capitalism, Socialism and Democracy* (Routledge 1942) 84.
[526] ibid 81–86.
[527] J Gregory Sidak and David J Teece, 'Dynamic Competition in Antitrust Law' (2009) 5 Journal of Competition Law and Economics 581, 600. In the words of Schumpeter, "[t]he introduction of new methods of production and new commodities is hardly conceivable with perfect –and perfectly prompt- competition from the start… [T]his means that the bulk of what we call economic progress is incompatible with it… [p]erfect competition is not only impossible but inferior, and has no title to being set up as the model of ideal efficiency..." Schumpeter (n 526) 105-106.
[528] David J Teece, *Managing Intellectual Capital: Organizational, Strategic, and Policy Dimensions* (OUP 2000) 160–163.

serious challenger. As a result, consumers suffer anticompetitive effects in the form of reduced competition, lower levels of innovation[529] and limited consumer choice.

In particular, achieving sufficient scale quickly is the main goal of any data-driven firm entering a market. However, Facebook's nowcasting radar effectively prevents newcomers from achieving a scale that is anywhere near to one capable of posing a threat to Facebook, since as soon as a nascent competitor is becoming popular, Facebook gives it a binary choice: either be acquired or be squashed. If an entrant is brave enough to resist an acquisition offer and chooses instead to compete with Facebook, it is very likely that Facebook will steal the entrant's innovation, leverage its user base and make even more profit that the entrant would have otherwise made.[530] The prospect of becoming a target can chill start-ups' incentives to compete and innovate in segments and ways that may potentially threaten Facebook's market power.[531] As a consequence, competition and innovation levels are lowered in the areas where Facebook has presence. As a monopolist, Facebook has no incentive to continue innovating in the social network market. Indeed, in the 2016 F8 conference, Mark Zuckerberg laid out in detail a long-term vision for the areas where Facebook was determined to innovate; conversely, after the realisation that Facebook could just copy Snapchat's features and leverage its network to squash it, in the 2017 f8 conference 'there was no vision, just the wholesale adoption of Snap's [innovations], plus a whole bunch of tech demos that never bothered to tell a story of why they actually mattered for Facebook's users.'[532] Moreover, Facebook's products and services, even if inconsistent with the preferences of some consumers, become the only available options. For example, when Facebook acquired WhatsApp in 2014, WhatsApp's business model was not designed for fast revenue growth, only user growth. Its business model was simple: the provision of a free service for a year and charging an annual 1-dollar subscription fee thereafter. Crucially, WhatsApp's founders had an aversion to adopting an advertising model for a social messenger service, because they were especially committed to protecting user privacy given the 2013 mass surveillance revelations in the Edward Snowden affair. However, after WhatsApp's acquisition by Facebook, the latter amended WhatsApp's privacy policy to allow data to be shared with Facebook,[533] thereby effectively limiting the options of those consumers who prefer higher levels of data protection.

IV. REMEDIES

Given that each type of anticompetitive conduct by Facebook is a manifestation, or symptom, of one single illness, the best course of action is to adopt an array of measures on different yet related fronts that together would serve as an antidote to Facebook's unrestricted ability and incentive to collect and process data.[534] A positive aspect of this

[529] Commenting on Facebook's tactics enabled by Onavo, Ashkan Sotani observed: '[e]ssentially this approach takes data generated by consumers and uses it in ways that directly hurts their interests — for example, to impede competitive innovation.' Seetharaman and Morris (n 488).
[530] See text accompanying footnote 499.
[531] Stucke (n 506) 307.
[532] Ben Thompson, 'Facebook and the Cost of Monopoly' (*Stratechery by Ben Thompson*, 19 April 2017) <https://stratechery.com/2017/facebook-and-the-cost-of-monopoly/>.
[533] Tas Bindi, 'WhatsApp, Facebook to Face EU Data Protection Taskforce' (*ZDNet*, 27 October 2017) <https://www.zdnet.com/article/whatsapp-facebook-to-face-eu-data-protection-taskforce/>.
[534] According to Andreas Mundt, to tackle the market power of Internet giants, the solution may be for regulators worldwide to impose remedies around data use and access. Michael Acton, 'Google, Facebook and Other "Internet Giants" Should Face Breakup of Market Power in the Long Run Mundt Says'.

approach is that it is likely to generate a 'virtuous cycle' for consumers and society as a whole. Improved online privacy and due respect for consumers' data protection rights, on the one hand, coupled with the mitigation of information asymmetries, enhanced transparency and consumer education, on the other hand, are likely to reduce the scope of Facebook's data collection operations (and therefore the extent of its data advantage) and lower barriers to entry for privacy-driven services. Improvements in competition can be furthered reinforced by specific 'traditional' competition policy remedies such as interoperability obligations coupled with effective data portability, and a requirement that Facebook's social algorithms stop prioritising traffic within its properties, to the detriment of other websites, especially news outlets. These remedies, in turn, would prevent the dissemination of news stories which are wholly made up and created to drive traffic and generate advertising revenues, and therefore the scope of political manipulation and misinformation enabled by Facebook's services would be reduced. Crucially, these remedies have the potential to halt the propagation of the surveillance capitalism business model that is spreading across the Web at a dramatic pace.

The combination of measures that is being proposed must be implemented immediately, as the costs consumers and society are paying are already too high, and continue on the rise. However, additional measures must be implemented in competition policy to ensure beneficial outcomes in the long run. Guided by the extremely narrow consumer welfare benchmark, antitrust and merger policy have failed to curb market power, prevent concentration and keep online markets opens and contestable. Accordingly, an overhaul of antitrust doctrine, which entails a departure from the current excessive emphasis placed on price and output, a focus on the competitive process and market structure, and certain improvements to merger control are warranted.

A. Curbing Facebook's Ability and Incentive to collect Data

1. Ability

Facebook's ability to collect data can be readily and significantly reduced based on strong enforcement of the GDPR, especially in relation to the need to obtain users' valid consent to process personal data and the observance of the purpose limitation and data minimisation principles.

For consent to serve as legal basis to legitimise the processing of personal data, it must be freely given, specific, informed and unambiguous. These requirements were assessed in Section III.A.3.

Article 5(1)(b) of the GDPR provides that personal data must be 'collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […] ('purpose limitation')'. The purpose limitation principle is intended to place the boundaries within which personal data for a given purpose may be processed and subsequently used, thereby inhibiting 'mission creep'[535] and consequently undue interferences with people's data protection rights.

[535] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 00569/13/EN WP 203 4.

This principle has two main components: 'purpose specification', and 'use limitation' or 'compatible use'. Purpose specification requires that the purpose or purposes of the data collection be clearly and specifically identified, prior to and no later than the time at which the personal data collection takes place, with sufficient detail to determine what kind of processing falls or does not fall within the scope of the specified purpose. Accordingly, vague or general purposes such as 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' are normally insufficient to meet the 'specific' criterion.[536] When data processing take place in complex, opaque and ambiguous contexts, especially on the Internet, 'special care is needed to unambiguously specify the purposes.'[537]

In turn, the notion of compatible use requires that any further processing subsequent to data collection, whether for purposes initially specified or for any additional purposes, must be compatible with the initial processing. It corresponds to the idea that the data collected about individuals will not be used by the entity collecting the data outside the realm of reasonability.[538] Compatibility is determined on a case-by-case basis based on substantive criteria such as the context in which the data has been collected, the reasonable expectations of the data subjects as to its future use and the nature of the data. The more unexpected or surprising the data's subsequent use is, the more likely it is that the further use will be considered incompatible.[539] The Article 29 Working Party provides a good example in this connection:

'A market-leading social networking and photo-sharing site allows its users to upload photos for personal use and share them with selected 'friends'. The privacy notice reassures customers that the photos will only be shared 'with whom you want, when you want'. Two years later, the company changes its privacy policy. In an email it notifies its customers that a new privacy policy will come into effect and unless they remove their photos within 30 days, they will be deemed to have consented to giving the site a license to use all uploaded photos for any purpose, including, but not limited to, promotion of the website. A detailed license agreement and privacy policy are provided in a link to the email as well as via the site whenever the customer visits it. The customer must accept these documents by clicking 'I accept' before being allowed to continue browsing the website. This further use of the photos - besides raising other data protection concerns such as validity of the consent, proportionality, and legitimacy - also raises compatibility issues. The change clearly could not have been expected by the customers who have by now uploaded two years' worth of their photos online with the understanding that they will only be shared 'with whom [they] want, when [they] want'. The purpose of the initial processing (allowing customers to share their photos with their friends) is clearly unrelated to the - excessive - further use by the company. The context and the specific assurances given in advertising the services at the time of the initial collection also confirm the assessment of incompatibility.'[540]

Also, the balance of power between the data subject and the data controller must be taken into account. Compatibility of further processing will be unlikely if the data subject is not given sufficient freedom of choice, if the terms of any involved consent were unspecific, and if the further use is deemed objectionable.[541] Moreover, the more sensitive the

[536] ibid 16.
[537] ibid 18.
[538] Ghosh and Scott (n 29) 32.
[539] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (n 536) 24.
[540] ibid 60.
[541] ibid 24.

information involved is, such as biometric data, location data and other types of information requiring special protection, the smaller is the room for compatibility.[542] Continuing with the Article 29 Working Party's example:

'The nature of the data is also a factor that supports incompatibility: although many of the photos uploaded on the site might be innocuous, others can be more intimate, perhaps embarrassing, or simply badly taken. They can also be misinterpreted, if taken out of context. Further, the thought that the photos may be used for promotional or other purposes may have a stifling effect of self-censorship on what people might post on the website, which could be classed as a potential impact on the data subject. The balance of power between the consumers and the photo-sharing website, and lack of suitable alternatives for photo-sharing services, may also contribute to the conclusion that consent alone, collected in this form and under these circumstances, is unlikely to be sufficient to compensate for this excessive and unexpected change of purpose.'[543]

Moreover, Article 5(1)(c) of the GDPR provides that personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').' Accordingly, this principle forces data controllers to collect and keep only the personal data they need to achieve their purpose, and not more. As a consequence, personal data may not be collected on the off-chance that it might be useful in the future, for whatever purposes.

Facebook is a notorious recidivist offender of EU data protection law. As seen in Section III.A.3, its approach to elicit consumer consent is insufficient to meet the freely given, informed, specific and unambiguous criteria. In addition, it has routinely violated and continues violating the purpose limitation principle. As seen in Section II, Facebook has mastered the strategy of making privacy promises that have an appeal to consumers in its Data Policies and subsequently rolling back on those promises for financial gain. Also, the manner in which Facebook explains the purposes for which it collects personal data is vague and confusing, and oftentimes the relevant information is misleading and difficult to find. Based on the information Facebook provides in its Data Policy, it is not possible to determine the specific kind of data that is used for a specific purpose (for instance, for targeted advertising or the provision of analytics and other services or 'research and innovation for social good'), let alone to what specific 'business partners' or 'Facebook companies' the data may be shared for further processing. Any personal data collected on Facebook, for example, may be shared to and used in Instagram or WhatsApp, for whatever purposes stated in the privacy policies of the last two services. Moreover, Facebook's data processing operations violate its users' reasonable expectations as to the further uses of their personal data. Reasonable users surely expect some extent of data processing for the provision of the social networking experience and targeted advertising on Facebook, as the service is zero-priced. However, they are unlikely to have expected that their data could be collected across thousands of apps and websites across the Internet and used for behavioural advertising and location-based advertising off Facebook. The use of click-wrap agreements and the overwhelming imbalance of power between Facebook and its users, based on which it imposes abuses terms on its users and elicits forced consent for the processing of users' personal data, confirm the view that Facebook's data processing practices fail to meet the compatible use requirement. The fact that Facebook has been found to have processed sensitive data such as sexual orientation to provide

[542] ibid 25.
[543] ibid 61.

targeted advertising reinforces this view even further.[544] Last but not least, the amount of data that Facebook collects based on the use of its services, including permanent location and browsing behaviour tracking, and the combination of data from different sources into detailed user profiles, is incompatible with the data minimisation principle.

If Facebook were forced to obtain actually valid consent for the processing of its users' personal data and abide by the two principles described above, the scope of its data advantage, and consequently the magnitude of its data-driven market power, would be significantly reduced.

Facebook's source of market power and commercial success is directly correlated with the amount of data it is able to collect. The more data at its disposal, the greater will be the scope of improvement for its social and ad targeting algorithms.[545] Indeed, as acknowledged by Facebook's chief financial officer, less data is directly correlated with lower advertising revenues.[546] If users gave valid consent, as opposed to forced consent, they would be duly informed as to the specific kind of data that Facebook collects for the provision of its services, and would be able to deny that consent if they considered some type of data collection intrusive or inconsistent with their privacy preferences, without fear of being forced to close their accounts. The possibility of consenting to the data collection necessary for the provision of Facebook's services, whilst still having the possibility to deny consent to intrusive data processing operations that only seek to increase Facebook's profitability, would be in and of itself sufficient to put an end to the exploitative abuse explained in Section III.A.

Given users' attitudes to online advertising seen in Section II.A., it is likely that a big portion of users would significantly reduce the scope of their consent to Facebook's data processing operations, especially the collection of browsing data off Facebook. Therefore, Facebook's stream of data could be drastically reduced. In addition, respect of the purpose limitation principle would mean that Facebook could not leverage its data advantage into other segments. For example, the data gathered on Facebook for the improvement of social interactions could not be used for adverting or other purposes on Instagram or on websites and apps members of the Audience Network. Nor could Facebook combine data from different sources, such as Instagram, Messenger, Facebook and WhatsApp, to enrich its user profiles, since users could not reasonably expect the processing of their personal data in this way.[547] Respect for the data minimisation principle would in turn mean that Facebook could only collect the data that is strictly necessary for the provision of its social networking and messaging services, and not the data that is craves for its wider business model.

---

[544] Dutch DPA, 'Conclusions of Final Report of Findings about the DPA's Investigation into the Processing of Personal Data by the Facebook Group, 23 February 2017' (2017) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_facebook_february_23_2017.pdf>.

[545] ' [P]latforms are designed to extract as much personal information as possible from users in order to optimize the curation of organic content and the targeting of ads. The less privacy a user has from the platform, the more precisely the algorithms can target content.'. Ghosh and Scott (n 29) 22.

[546] See text accompanying footnote 256.

[547] "[T]his is what many users are not aware of: Among other conditions, private use of the network is subject to Facebook being able to collect an almost unlimited amount of any type of user data from third party sources, allocate these to the users' Facebook accounts and use them for numerous data processing processes." Bundeskartellamt (n 87) 3.

Given that the idea is to reduce the scope of Facebook's data collection operations, Facebook should be bound to uniformly respect the principles and requirements above in as many jurisdictions as possible. The GDPR contemplates suitable mechanisms to ensure uniform enforcement across the EU. Where a significant number of data subjects in several Member States are likely to be substantially affected by processing operations, as in the case of Facebook's operations, the *Data Protection Authority* (DPA) of each of those Member States have the right to participate in joint investigations and joint enforcement measures.[548] Accordingly, a task force comprising all of the DPAs of the EU could be set up to investigate the scope of Facebook's data processing activities, determine infringement of the GDPR as described above, and impose an appropriate fine and remedies on Facebook. Following the procedure set out in Article 60 of the GDPR, the DPAs can reach a single binding decision. Upon notification of this decision by the lead DPA to Facebook, the latter would be bound to take all such necessary measures to ensure compliance with the decision with regard to its processing activities in the context of all its establishments in the Union.[549] The joint decision can order Facebook to bring its processing operations into compliance with the provisions of the GDPR, in a specified manner and within a specified period,[550] impose a temporary or definitive limitation, including a ban on processing,[551] and/or impose an administrative fine of up to EUR 20,000,000 or up to 4% of Facebook's total worldwide annual turnover of the preceding financial year.[552]

Stronger enforcement of the consumer protection rules can also contribute to limit the extent of Facebook's data-driven market power. Section III.B.2 explained that one of the consequences of Facebook's misleading commercial practices and omissions is that, motivated by a poor understanding of Facebook's data collection practices and privacy settings resulting from deception, users disclose more personal data than they intend, and congruently Facebook can access more data to strengthen its dominant position in the social network market and reinforce its position in the display advertising segment. Thus, the elimination of the mechanisms and techniques through which Facebook deceive consumers into disclosing personal data in a manner contrary to their privacy preferences and nudge consumers to stick to privacy-intrusive settings are indispensable measures to reduce the extent of Facebook's data collection, and therefore of its data-driven market power.

Some consumer protection authorities have made laudable efforts to stop Facebook from continuing engaging in these practices. For example, the Italian *Autorita Garante della Concorrenza e del Mercato* (AGCM) imposed a EUR 3 million fine on Facebook for having deceived consumers into wrongly believing that they had to consent to the sharing of their personal data from WhatsApp to Facebook if they wished to continue using WhatsApp. According to the AGCM:

'this practice [was] implemented through: a) an in-app procedure for obtaining the acceptance of the new Terms of Use characterized by an excessive emphasis placed on the need to subscribe to the new conditions within the following 30 days or lose the opportunity to use the service; b) an inadequate information on the possibility of denying consent to share with Facebook the personal data on WhatsApp account; c) the pre-

[548] Article 62(1) and (2) GDPR.
[549] Article 60(10) GDPR.
[550] Article 58(2)(d) GDPR.
[551] Article 58(2)(e) GDPR.
[552] Article 83(5) GDPR.

selection of the option to share the data [… and]; d) finally, the difficulty of effectively activating the opt-out option once the Terms of Use were accepted in full.'[553]

A year later, the AGCM imposed a EUR 10 million fine on Facebook for exerting undue influence on registered consumers, who without giving express and prior consent, unwittingly transfer their personal data from Facebook to third-party websites/apps for commercial purposes, and vice versa. The undue influence arose from the pre-selection of settings that enabled the broadest consent to data sharing, and when users decided to limit their consent, they were confronted with cumbersome restrictions on the use of Facebook and third party websites/apps, which incentivised them to stick to the privacy-intrusive pre-selected choice. In particular, the AGCM held:

'Facebook pre-sets the ability of its users to access websites and external apps using their FB accounts, thus enabling the transmission of their data to the single websites/apps, without any express consent. Facebook then reiterates the opt-out pre-selection mechanism, with respect to data sharing, whenever users access third-party websites/apps, including games, using their Facebook accounts. In this case also, users can in fact only deselect the pre-setting operated by Facebook, without being able to make a free, informed choice.'[554]

If Facebook stopped nudging consumers into accepting data-sharing terms based on deceptive statements and coercion, privacy-sensitive consumers would expectedly choose the options that protect their personal data. Moreover, consumers tend to stick with the default setting instead of actively choosing an alternative or opting-out. Importantly, this seems to hold regardless of what the default is and what the decision concerns. [555] Accordingly, privacy settings that are pre-selected to the privacy-friendly option, as opposed to the privacy-intrusive one, are capable of having a big difference in terms of the volume of data a platform may collect. The imposition on Facebook of EU-wide obligations to show data-sharing options based on accurate, clear and concise information and to pre-select the options that disclose the least amount of personal data, congruently, has the potential to dramatically reduce the magnitude of its data-driven market power. The consumer protection authorities of the 28 Member States can resort to the *Consumer Protection Cooperation Network* (CPC Network) to collectively request the Irish consumer protection authority [556] to order Facebook to cease the relevant intra-Community infringements, prohibit Facebook from engaging in the practices above and impose fines in the event of failure to comply with the relevant decision, in accordance with Articles 4(6) and 8 of the Regulation on Consumer Protection Cooperation (the CPC regulation).[557]

---

[553] Autorità Garante della Concorrenza e del Mercato (AGCM), 'WhatsApp Fined 3 Million Euro for Having Forced Its Users to Share Their Personal Data with Facebook' (2017) <https://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html>.

[554] AGCM - Autorita' Garante della Concorrenza e del Mercato, 'Facebook Fined 10 Million Euros by the ICA for Unfair Commercial Practices for Using Its Subscribers' Data for Commercial Purposes' (7 December 2018) <http://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes>.

[555] OECD, 'Improving Online Disclosures with Behavioural Insights: Towards Better Outcomes for Consumers' (2018) Directorate for Science, Technology and Innovation Policy Note, 4.

[556] Facebook's European headquarters are based in Dublin.

[557] Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation) O.J. L 364/1 1.

The new CPC Regulation (EU) 2017/239,[558] applicable as of 17 January 2020, is expected to substantially improve coordinated procedures among national enforcers to combat bad practices that harm consumers in most or all EU countries (two-thirds of Member States or more, and two-thirds of EU population or more).[559]

2. Incentive

A substantial reduction of Facebook's incentive to collect data through any means, at any cost, requires increased awareness and proper understanding on the part of consumers of the scope of Facebook's data processing operations and the detrimental effects on online privacy arising from the use of its services. Currently, with the majority of consumers uninformed or confused about Facebook's data processing practices and their related privacy harms, Facebook feels little to no pressure to reduce the intrusiveness of its practices, in spite of consumers' voiced preference for more online privacy. As the CMA observes, 'if consumers are limited in their ability to make informed decisions and to challenge firms over the use of their data, this may mean that firms have limited incentives to compete over the protection they afford to consumer data.'[560]

Conversely, if the number of sophisticated consumers were high enough, their discontent about Facebook's data collection operations would provide potential competitors with an incentive to enter and potentially disrupt the social network market by offering currently unavailable levels of data protection of their preference. In turn, Facebook would feel the competitive pressure arising from entry and switching and likely be compelled to reduce the intrusiveness of its practices and offer data protection granularities in its services to retain custom. This is consistent with the essential role of availability of good information in the marketplace for the proper functioning of competition. As Vickers observes: '[c]ompetition cannot work effectively unless consumers are reasonably well informed about the choices before them. Uninformed choice is not effective choice, and without that there will not be effective competition'.[561] Put in other words, a reduction of information asymmetries would diminish Facebook's incentive to violate the data privacy of its users to reinforce its data-driven market power and render the social network market more contestable for privacy-driven offerings catering to the needs of privacy-sensitive consumers.

To reduce information asymmetries in the social network market, the provision of adequate and clear information about Facebook's business model is essential. In this connection, the recent agreement at which Facebook, the Commission and EU Consumer protection authorities arrived to clarify Facebook's use of data is a welcomed development.

---

[558] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 O.J. L 345/1 1.

[559] For example, when it is determined that a trader operating across the EU is engaging in unfair commercial practices, the Commission can notify the Member State authorities that a common action needs to be launched, and the relevant trader should be asked to comply with EU law. This will lead to quicker protection for consumers across the EU. Also, for the first time, consumer protection authorities will be able to accept traders' commitments to give remedies to the affected consumers. Importantly, the trader in question will have a one-stop-shop at EU level instead of different appreciations and costly proceedings initiated by enforcement authorities. European Commission, 'Ensuring Consumer Rights Are Properly Enforced - Revising EU Consumer Protection Cooperation' 3 <https://ec.europa.eu/info/sites/info/files/factsheet_ensuring_consumer_rights_en.pdf>.

[560] CMA (n 342) 106.

[561] John Vickers, 'Economics for Consumer Policy, British Academy Keynes Lecture (29 Oct. 2003)'.

The Commission reported that 'Facebook will introduce new text in its Terms [of Use] explaining that it does not charge users for its services in return for users' agreement to share their data and to be exposed to commercial advertisements. Facebook's terms will now clearly explain that their business model relies on selling targeted advertising services to traders by using the data from the profiles of its users.'[562] However, the implementation of this measure must be done correctly. Since only few consumers read online terms and conditions in full, information about Facebook's business model should be made available not only in its Terms of Use, but also in multiple places on its website and at different points during users' interaction with the platform, including with the aid of images, audio and video, when appropriate.[563]

Moreover, the mechanisms and techniques through which Facebook conceals its data processing operations[564] should be eliminated. The use of 'layered notices' can be very effective to this end, as they can provide key information to consumers about data processing operations in a concise and user-friendly manner, whilst also supplying more detailed information on the next 'layer' to those requiring further clarification.[565] For example, during the first interaction of a user with Facebook a pop-up window could show up with concise information about privacy settings and their implications for online privacy. The window could show two options such as 'explore privacy settings' and 'explore later', bearing in mind that privacy settings should be pre-selected to the most privacy-friendly option. Once within the privacy settings, a triangular danger icon could be displayed next to the options that entail public disclosure of personal data or disclosures to third parties. By clicking on this icon, the benefits (such as enhanced social interactions) but also the risks associated with the relevant setting can be highlighted. In addition, notices can provide users with tips to avoid privacy intrusions that may not be entirely obvious for certain users. For example, a triangular danger icon next to location settings could explain that when these settings are on, Facebook is able to track with astonishing precision all the movements of a given user, and combine this information with other data for advertising purposes.

Finally, the measures above can be complemented with awareness-raising campaigns. For example, in 2014 the Commission launched an EU-wide Consumer Rights Awareness Campaign, with an aim to increase general knowledge among traders and consumers of EU consumer rights that stem from national transposition of EU Directives. An array of information was made publicly available, and myriad events took place in designated locations across the EU with the participation of consumer authorities, consumer associations, business associations and other stakeholders.[566] A similar EU-wide campaign could be launched to raise awareness of the business model of and harmful consequences stemming from social networking sites and other data-driven platforms. The campaign could serve to educate consumers about behavioural biases and the adequate channels and mechanisms to exercise consumer rights online. Moreover, this campaign could be supplemented with events and activities conducted by data protection authorities in each

[562] European Commission, 'Press Release - Facebook Changes Its Terms and Clarify Its Use of Data for Consumers Following Discussions with the European Commission and Consumer Authorities' (9 April 2019) <http://europa.eu/rapid/press-release_IP-19-2048_en.htm>.
[563] As the OECD observes, '[i]n some scenarios, images, audio and video can more effectively convey information to consumers than even the most clear and simple text.' OECD, 'Improving Online Disclosures with Behavioural Insights: Towards Better Outcomes for Consumers' (n 556) 5.
[564] See Section III.B.1.(b).
[565] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (n 536) 52.
[566] European Commission, 'Consumer Rights Awareness Campaign' (2014) <https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=30149>.

Member State, which are bound to 'promote public awareness and understanding of the risks, rules, safeguards and rights in relation to [data] processing.'[567]

3. Spillover Effects

It stems from the above that adequate protection of Facebook users' data privacy and data protection rights, coupled with a significant reduction of information asymmetries, has the potential to render the markets for social networking services and display advertising more contestable. If implemented, both measures are capable of considerably reducing the scale of data Facebook can reach, as a result of which the precision of its algorithms would be blunted. Consequently, advertisers would have an incentive to advertise elsewhere, and Facebook's revenues would suffer. In turn, an impinged Facebook would likely attract entry into the social media market.

But the positive effects stemming from more privacy and transparency do not end there. Since Facebook would have access to significantly less data, its content-targeting algorithms would also lose precision.[568] Accordingly, Facebook's social algorithms would find it harder to target content that is manipulative or merely optimised to confirm pre-existing biases, and therefore the extent of filter bubbles and echo chambers would be reduced. In turn, the upholding of the purpose limitation principle and consent requirements would place significant constraints on non-purpose specific collections leading to data leakage to malicious actors.

B. Competition Remedies

Reducing Facebook's ability and incentive to collect data or share the data it collects? is the first step to reinvigorate competition in the markets for social networking services and display advertising. In parallel, the following remedies should be implemented.

1. Interoperability

When a new service can be integrated with a large digital platform, it holds a significant advantage over standalone competitors. As a consequence, market entry may effectively become impossible without that technical integration and access.

Interoperability, that is, the '[c]apability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units',[569] can be particularly suitable to boost competition in markets where direct network effects play an important role, such as the social media and electronic communications markets. It can be achieved through the provision of transparent and publicly accessible APIs giving access to the data and functionality needed for technical integration between technological components. For example, for messaging services, an interoperability obligation imposed on WhatsApp would mean that a WhatsApp user could send a message to his friends using Telegram

[567] Article 57(1)(b) GDPR.
[568] 'The less privacy a user has from the platform, the more precisely the algorithms can target content' Ghosh and Scott (n 29) 22.
[569] IGI Global, 'What Is Interoperability' <https://www.igi-global.com/dictionary/interoperability-medical-devices-information-systems/15494>.

without the need of switching services. Or in the context of social media, users of competing social networks such as Diaspora or LinkedIn could post messages on somebody's Facebook page directly without the need to create a Facebook profile. Accordingly, consumer lock-in could be significantly reduced, thereby lowering barriers to entry.

However, large platforms, including Facebook, have a natural incentive to restrict the use of APIs by third parties. These incentives can be anticompetitive in intent and effect, such as when a platform obstructs a downstream market to prevent the growth of an emerging competitor.[570] Others can be motivated by privacy and security concerns, such as for example cutting off third party access to user data through an API. For instance, Facebook has implemented significant changes as a response to the Cambridge Analytica scandal.[571] Some of these changes, however, such as Facebook's deprecation of 'publish_actions',[572] have caused significant negative impacts on new technology projects and start-ups.[573] The problem for competition authorities is to determine when an API restriction lessening interoperability is implemented for legitimate and not anticompetitive purposes. As seen above, Facebook has already invoked privacy and security considerations to promote its own interests.[574] In the context of remedies, interoperability obligations could be imposed on Facebook, under which Facebook would be forced to give access to APIs in a way capable of restoring competition and promoting entry.

It was seen in Section III.D that Facebook cut off apps like Vine, Voxer, MessageMe and Phhhoto access to an indispensable API to boost growth, which ultimately led to the demise of these apps. Probably to contain PR damage caused by the leakage of internal documents that show Facebook's intent to impair Vine, Facebook formally announced a policy change allowing competing apps to integrate on top of Facebook, irrespective of the replication of functionality.[575] Accordingly, competing apps can now access the Find Friends API and other viral distribution features, and developers can build without fear of straying too close to Facebook's functionalities.[576]

Whilst this policy change is a welcomed development, the type of interoperability that could fully open the social network market has not been implemented yet. Even though competitors can now access Facebook's Find Friends API, consumers are not able to take their social graph and use it on another social media platform. This is because the data a user can download through the Download Your Information functionality is not interoperable.[577] True interoperability would mean that users could download their social graph from Facebook and upload their list of friends onto other social network providers, so they can find their friends there. In this connection, some have advocated giving users ownership of their social graph, based on a Social Graph Portability and Interoperability Act. This measure could greatly boost competition in the social network market, since if

---

[570] See Section III.D.
[571] Josh Costine, 'Facebook Restricts APIs, Axes Old Instagram Platform amidst Scandals' (*TechCrunch*, 2018) <http://social.techcrunch.com/2018/04/04/facebook-instagram-api-shut-down/>.
[572] Josh Costine, 'Facebook Shuts down Custom Feed-Sharing Prompts and 12 Other APIs | TechCrunch' (2018) <https://techcrunch.com/2018/04/24/facebook-api-changes/>.
[573] See for example Buffer, '[Publish] Facebook Profiles Can No Longer Be Connected to Buffer Publish - Buffer FAQ' <https://faq.buffer.com/article/985-publish-facebook-api-changes>.
[574] See text accompanying footnote 467.
[575] Josh Costine, 'Facebook Ends Platform Policy Banning Apps That Copy Its Features' (*TechCrunch*, 2018) <http://social.techcrunch.com/2018/12/04/facebook-allows-competitors/>.
[576] ibid.
[577] See paragraph containing footnote 418.

users can find their online connections on different social networks, they will be more likely to try new social network providers.[578] In turn, if newcomers know that they can attract existing Facebook customers, new social networks are more likely to emerge, the strength of network effects are lowered, and incentives to compete and innovate are promoted. As tech journalist Josh Constine observes:

'If you can't take your social graph with you, there's little chance for a viable alternative to Facebook to arise. It doesn't matter if a better social network emerges, or if Facebook disrespects your privacy, because there's nowhere to go. Opening up the social graph would require Facebook to compete on the merit of its product and policies. Trying to force the company's hand with a variety of privacy regulations won't solve the core issue. But the prospect of users actually being able to leave would let the market compel Facebook to treat us better.'[579]

Finally, interoperability can be an effective remedy in merger control. When the merging firms offer software or services that can be technically integrated in terms of data sharing or functionalities, the extent of the integration may change after the merger. Logically, the merged entity will explore the efficiencies and benefits that could ensue from increasing the degree of integration, and even lie about integration possibilities during the merger review.[580] The merging firms can decide to integrate through private APIs that offer limited interoperability by design, thereby effectively denying actual and potential competitors access to the merged entity's ecosystem. To avoid this outcome and the proliferation of walled gardens, as a condition for approving the merger the merged entity could be forced to make available the relevant APIs that enable integration to third parties under fair, reasonable and non-discriminatory terms. For example, in the context of the Facebook/WhatsApp merger, the merged entity could have been required to implement the mechanisms used to exchange data and communicate between Facebook and WhatsApp through transparent and accessible APIs. In this way, the prospect of future competition could have been preserved. Third parties could have been able to negotiate with the merged entity benefits such as data sharing or preferential embedding into user interfaces. Also, non-competition benefits could have ensued, as researchers could have had access to the same interfaces, and privacy advocates could have used them to identify, test and record how much information exchange takes place.[581] Crucially, the 'combined entity would still be able to realize the positive business benefits of integration—just not to the exclusion of others. And antitrust authorities could be brought in later should the platform operator be unreasonable and anticompetitive in how it offers access to its APIs and underlying data.'[582]

---

[578] Luigi Zingales and Guy Rolnik, 'Opinion | A Way to Own Your Social-Media Data' *The New York Times* (20 January 2018) <https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html>.
[579] Josh Constine, 'Facebook Shouldn't Block You from Finding Friends on Competitors' (n 418).
[580] After the Facebook/WhatsApp merer, the Commission fined Facebook for providing misleading information as to the possibility of integrating WhatsApp and Facebook datasets. European Commission, 'Press Release - Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover' (*European Commission*, 18 May 2017) <http://europa.eu/rapid/press-release_IP-17-1369_en.htm>.
[581] Chris Riley, 'Competition through Interoperability' (*Chris Riley*, 6 October 2017) <https://medium.com/@mchrisriley/competition-through-interoperability-3ed34a5c55f1>.
[582] ibid.

2. Data Portability

In close connection and combination with the above, data portability obligations have the potential the restore competition in the social network market.

Article 20 GDPR enshrines the right of data subjects 'to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.' This right to data portability, which includes the right to request that 'personal data are transmitted directly from one controller to another, where technically feasible', has a competition policy dimension, as it is intended to reduce lock-in effects and switching costs for consumers. Indeed, the right to data portability is partly premised on the idea that consumers have low incentives to switch providers once they have invested their persona data on a specific platform, a salient phenomenon in the market for social networks. As Graef observes: '[t]he fact that the numerous changes made to the privacy policies of social networks like Facebook have not led to a direct decline in activity in spite of the fierce opposition that these changes have sometimes caused on the part of the users, may form an indication of the high degree of lock-in in online social networks.'[583]

The problem with the right to data portability is that in only applies to personal data that has been 'provided' to the controller by the data subject. Accordingly, non-personal data such as anonymised data or even metadata is excluded from the scope of this right. In addition, personal data that has been uploaded to a social network by a user other than the data subject also falls outside the scope of application of this right. Therefore, the right to data portability is of difficult application in the context of social networks, for which reason its beneficial effects on competition have been called into question.[584]

However, the rationale of Article 20 GDPR could be used to enter into a behavioural commitment with Facebook in order to promote competition. The scope of applicability of Article 20 GDPR could be extended to non-personal data and data about the data subject provided by other users in order to enable meaningful porting of profiles and other information onto competing social network providers. This measure 'would make data portability more meaningful and effective when a social network is market dominant,'[585] as Facebook users would have the real possibility to keep and transfer all the information they have gathered over the years on Facebook to other social networking platforms. Yet, this remedy is bound to be ineffective insofar as the necessary degree of interoperability between social networks is missing. As Vanberg and Unver explain: 'users are uninterested in pure data export, as it is a complex and time-consuming process, with inherent uncertainty, as the data transferred may not be utilised by other data controllers due to technical and architectural constraints.'[586] If the user data gathered from Facebook cannot be used elsewhere, there will be no incentives to switch. Therefore, interoperability and data portability must go hand in hand. To this effect, technical standards should be adopted

[583] Inge Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union' (2015) 39 Telecommunications Policy 502, 508.
[584] Graef (n 584).
[585] Marco Botta and Klaus Wiedemann, 'EU Competition Law Enforcement Vis-À-Vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita' [2018] Max Planck Institute for Innovation and Competition Research Paper No. 18-08 86.
[586] Aysem Diker Vanberg and Mehmet Bilal Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' (2017) 8 European Journal of Law and Technology 10.

to enable the seamless transmission of data between social network providers and ensure a level playing field for small operators and entrants.

An alternative to data portability coupled with interoperability is mandated data sharing. To counter the strong network effects and data-driven externalities that characterise certain online markets, some scholars are arguing that mandated data sharing is essential to promote competition in digital sectors. According to Pruffer and Schottmuller: '[b]y increasing access to […] anonymized clickstream data, other parties in different markets can use them for further innovation. At the same time, a strong concentration of large internet companies on these markets can be avoided.'[587] The idea is that access to the incumbent's data by competitors is likely to enable them to innovate and improve their services, compete on the merits and reduce the extent of the incumbent's data advantage. It is highly likely that this approach can lead to positive competitive outcomes. However, it lies in tension with data protection considerations.

By demonstrating feasibility of large-scale re-identification using movie-viewing histories and in general any behavioural or transactional profile, Narayanan and Shmatikov have proved that 'once any piece of data has been linked to a person's real identity, any association between this data and a virtual identity breaks the anonymity of the latter.'[588] Therefore, if anonymisation cannot be properly achieved, mandated data sharing is likely to cause significant privacy harms far beyond those Facebook has already caused, as anonymised information that is in the exclusive possession of Facebook could be made available to a potentially large number of rivals, which may be able to de-anonymise the data with relative ease.[589] Hence, insofar as no technical mechanisms exist to ensure the anonymity of data, this measure should be avoided.

3. Fair and Non-discriminatory Content Algorithm

It was seen in Section III.C that Facebook has tweaked its social algorithms to prioritise content that keeps users on the platform, in a move to increase user engagement and therefore have access to more data to fuel its virtuous cycle, thereby harming competitors who are dependent on Facebook's traffic referrals.

Accordingly, Facebook should be prevented from implementing any modifications to its news feed algorithms that result in advantages for the platform and harms for rivals. In

---

[587] Inge Graef and Jens Prufer, 'Mandated Data Sharing Is a Necessity in Specific Sectors' (2018) 103 Jaargang 298.

[588] Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets', *in 2008 IEEE Symposium on Security and Privacy (SP 2008)* (IEEE Computer Society 2008) 9 <http://ieeexplore.ieee.org/abstract/document/4531148/>.

[589] For example, in 2006 AOL made public over 20 million search queries made by thousands of subscribers over a three-month period. After replacing the subscribers' names or user IDs with identification numbers to protect the searchers' anonymity, AOL posted the data for research purposes. The data connected the 'anonymised' AOL member with his or her search queries, the number of websites identified by AOL's search engine as responsive to the search queries, and the resulting website the individual chose to visit. Based on this information, the New York Times was able to identify one subscriber named Thelma Arnold: 'search by search, click by click, the identity of AOL user No. 4417749 became easier to discern… It did not take much investigation to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs.' Michael Barbaro and Tom Zeller, 'A Face Is Exposed for AOL Searcher No. 4417749' (*The New York Times*, 2006) <http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=1&_r=1>.

particular, Facebook's algorithms should subject every type of content, regardless of whether it fuels traffic within Facebook or leads to traffic being referred to third party websites, to the same underlying processes that have an impact on the content's visibility and ranking on Facebook's news feeds.

To this effect, a system of independent review of Facebook's algorithms should be devised and implemented. For example, a team of expert auditors could regularly review the operation of such algorithms, examine the data that is used to train them, and determine the potential for bias in the rankings and promotion of content. This would allow auditors to run controlled experiments over time to determine if the algorithms subject to review are leading to competitive advantages for Facebook in the form of increased traffic, or whether there is discriminatory treatment for publishers' content. Although this idea is new and untested, so too were once upon a time 'the wild-eyed notions of independent testing of pharmaceuticals and the random inspection of food safety.'[590] Moreover, scholars such as Ezrachi and Stucke have advocated an algorithm auditing regime in the context of algorithmic collusion.[591]

C. Departure from the Narrow Consumer Welfare Standard and more Emphasis on the Competitive Process and the Openness of Markets

To a great extent Facebook's entrenched and growing dominance has been enabled by the dramatic change in competition policy that took place in the 70s and 80s. Currently, competition policy is excessively fixated with competitive outcomes that yield benefits to consumers in the form of low prices. In this light, Facebook and other online platforms like Google and Amazon are seen as examples to follow. However, this approach to competition policy has proved incapable of protecting competition and preventing excessive concentration in online markets. Therefore, another change in antitrust doctrine is required to capture and control the dynamics of market power in data-driven sectors.

Throughout the decades following the Second World War and particularly during the 1960s and 1970s, the United States courts and agencies adopted the economic theories of a group of Harvard scholars[592], who broadly speaking argued that large-scale enterprises were not behaving in furtherance of the public interest. From an economic perspective, the hitherto dominant structural doctrine argued that when only a few firms competed in an industry, those firms would readily find a way to mute their rivalry and exercise market power, thereby harming buyers.[593] Monopolistic and oligopolistic market structures enabled dominant market operators to easily and readily fix prices, divide markets and engage in tacit collusion. Also, monopolistic and oligopolistic undertakings were able to abuse their dominance to prevent entry, and to leverage their greater bargaining power against customers and consumer to profitably raise prices and degrade quality, without the

[590] Ghosh and Scott (n 29) 20.
[591] Ariel Ezrachi and Maurice E Stucke, 'Two Artificial Neural Networks Meet in an Online Hub and Change the Future (Of Competition, Market Dynamics and Society)' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2949434 34 <https://papers.ssrn.com/abstract=2949434> accessed 4 June 2019.
[592] The Harvard scholars included Donald. F. Turner and Philip Areeda, who were influenced by earlier Harvard economists such as Edward Chamberlain and Edward Mason, to name a few. Herbert Hovenkamp, "The Rationalization of Antitrust, 116 Harv. L. Rev. 917-920 (2003)
[593] Andrej Fatur, "EU Competition Law and the Information and Communication Technology Network Industries : Economic versus Legal Concepts in Pursuit of (Consumer) Welfare" (Harsh Publishing Limited, 2012), 33.

fear of consumer switching. Moreover, not only were market concentration and large firms seen as threats to consumers and buyers, but also to small businesses,[594] given that they limited their ability and freedom to compete.

The structural view of competition was the underpinning of vigorous competition enforcement. Courts and competition enforcement agencies regularly saw as anticompetitive any agreements and practices the effect of which was to enhance, obtain or exercise market power by firms, irrespective whether the conduct subject to scrutiny had the potential of benefiting consumers through lower prices or increased output.[595] Horizontal and vertical mergers leading to anticompetitive market structures and market foreclosure were almost certain to be blocked. In the 1968 Merger Guidelines barriers to entry, concentration, and large-scale firm dominance were the primary areas of concern for the competitive process.[596]

The Chicago School, the teachings of which became the mainstream approach to antitrust in the 70s and 80s, challenged the structuralist view. It espoused price theory as the 'proper lens for viewing antitrust problems',[597] and its insights were informed by a blind faith in the efficiency of markets and their self-correcting forces. Market players were seen as rational economic actors seeking to maximise profits in the most efficient manner. As a result, practices that had an efficiency explanation were seen as plausibly procompetitive, which led to a lax, laissez-fair competition policy concerned with the avoidance of false positives. According to the Chicago School, 'predatory pricing, vertical integration and tying arrangements never or almost never' were conducive to competition problems.'[598] Critically, the Chicago School advanced the maximisation of consumer welfare, through the promotion of economic efficiency,[599] as the exclusive normative goal of antitrust, a view endorsed by the US Supreme Court in 1979 when it held that 'Congress designed the Sherman Act as a "consumer welfare prescription"'.[600] Consumer welfare is measured through effects on consumer prices and output levels, with the consequence that other 'unmeasurable' considerations such as quality degradations, impairment of choice or reduced innovation play a secondary role.[601] Accordingly, competition enforcement is only triggered when a clear harm to consumer welfare can be established in the form of price increases or output reductions. The prescriptions of the Chicago School were soon followed in other jurisdictions, including the EU. Indeed, the review of the enforcement approach to Article 102 TFEU launched by the Commission in 2005 and the ensuing 2009 *Guidance on Enforcement Priorities* were marked by a preponderant focus on consumer welfare.[602]

---

[594] See for example Brown Shoe Co. v. United States, 370 U.S. 294 344 (1962), were was argued the promotion of competition through the protection of viable, small, locally owned business. Thus, a merger which decreased the costs of a firm thereby injuring small competitors should be condemned.

[595] Thomas A Piraino Jr., "Reconciling the Harvard and Chicago Schools: A New Antitrust Approach for the 21st Century", Indiana Law Journal: Vol. 82: Iss. 2., Article 4, 346.

[596] U.S. Department of Justice, '1968 Merger Guidelines' (1968) <https://www.justice.gov/archives/atr/1968-merger-guidelines>.

[597] Richard A Posner, 'The Chicago School of Antitrust Analysis' (1978) 127 U. Pa. L. Rev. 925, 932.

[598] Daniel A Crane, 'The Tempting of Antitrust: Robert Bork and the Goals of Antitrust Policy' (2013) 79 Antitrust LJ 835, 852.

[599] Robert H Bork, *The Antitrust Paradox: A Policy at War with Itself* (First Edition edition, Free Press 1993) 7, 405.

[600] Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979)

[601] A critique of this approach can be found in for example Tim Wu, *The Curse of Bigness Antitrust in the new Gilded Age* (Columbia Global reports, 2018).

[602] European Commission, Guidance on the Commission's Enforcement Priorities in Applying Article [102 TFEU] to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C 45/7, para 19.

The current competition doctrine has failed to promote competition, especially in data-driven markets. Given consumer welfare's narrow focus on prices, conduct and mergers that impinge upon non-competition parameters are highly likely to be unpunished or approved. Moreover, the excessive focus on consumer welfare is inconsistent with legislative history in both the US and the EU, since in both jurisdictions the competition laws were influenced by and enacted to protect a number of political and economic goals. Finally, it erroneously replaced a concern about process and structure (i.e. whether market structure is capable of supporting a competitive landscape) with a normative value as to what is a positive outcome (i.e. whether consumers are better off).[603]

An undertaking that limits consumers' choices is likely to be as or even more harmful to consumers than other firms that raise prices. A determination of whether or not consumer welfare has been harmed as a result of price rises as a precondition to trigger antitrust liability fails to capture the fact that undertakings also compete on the basis of non-price facets of competition such as quality, choice and innovation, and that consumers are equally harmed whenever any of said facets is negatively affected.

For example, none of Facebook's abuses of dominance detailed in Section III has had a negative effect on prices, as Facebook offers its platform services at a zero price on the user side. For some, zero prices and harm to consumers are mutually exclusive. For instance, Wright and Manne have argued that 'it's really hard to see the above-marginal-cost pricing in these [digital] markets. From the point of view of the buyers… these monopolists are really pathetic at extracting profits, as most of them give away their products for free…'[604] Yet, it was seen that Facebook's set of anticompetitive practices has had nefarious effects on consumer choice, quality and innovation.[605] Put in other words, the potential harms to competition posed by Facebook's dominance and conduct escape the antitrust radar if competition is primarily assessed through price and output. The fact that negative effects on non-price competition parameters are not as readily measurable as price increases should not justify a dismissal of the former effects and an excessively preponderant role of the latter.[606]

In addition, the primary focus on price and output renders competition enforcement ineffective, as intervention is delayed until market power is actively exercised, with utmost disregard for market structure and the competitive process that led to such market power.[607] As a result, enforcers are likely to overlook the structural weakening of

---

[603] Lina M Khan, 'Amazon's Antitrust Paradox' (2016) 126 The Yale Law Journal 564, 737.
[604] Joshua Wright and Geoffrey Manne, 'What's An Internet Monopolist? A Reply to Professor Wu' (*Technology Liberation Front*, 23 November 2010) <https://techliberation.com/2010/11/23/whats-an-internet-monopolist-a-reply-to-professor-wu/>.
[605] See generally Section III.
[606] When accepting his Nobel Prize for economics, Friedrich Hayek famously criticised those who: "…happily proceed on the fiction that the factors which they can measure are the only ones that are relevant." In particular, he stated: "We know: of course, with regard to the market and similar social structures, a great many facts which we cannot measure and on which indeed we have only some very imprecise and general information. And because the effects of these facts in any particular instance cannot be confirmed by quantitative evidence, they are simply disregarded by those sworn to admit only what they regard as scientific evidence: they thereupon happily proceed on the fiction that the factors which they can measure are the only ones that are relevant." Frederich August von Hayek, 'The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 1974' (*NobelPrize.org*) <https://www.nobelprize.org/prizes/economic-sciences/1974/hayek/lecture/>.
[607] Khan (n 604) 738.

competition until it becomes hard to address effectively.[608] This is largely the result of the Chicago School's hostility to false positives and the belief that market power and high concentration can produce efficient outcomes.[609] Accordingly, significantly greater consideration to false negatives, non-price parameters of competition and a focus on a solid competitive process and open markets should be the first steps to restore competition law's ability to promote competition in online platform markets.

Moreover, the idea that consumer welfare is the sole goal of antitrust betrays the legislative history of and values that informed the competition laws in both the US and the EU.

The framers of the *Sherman Act*, the first competition statute in the world, saw classical economic values and libertarian political values as closely connected and dependent on each other: the Act was a means to protect natural rights to economic liberty, security of property and the process of competitive, free exchange from artificial distortions.[610] The *Sherman Act* was passed out of a concern for the power and exploitative conduct of large and powerful business organisations named trusts, and it was intended to rein in their power.[611] As a response to a fear of concentrations of power, antitrust sought to distribute it.[612] Importantly, the *Sherman Act* was underpinned by the conviction that concentration of economic power results in the consolidation of political power, thereby engendering antidemocratic political pressures and undermining individual and business freedom.[613] Thus, the dispersion of both economic and political power was a paramount goal. Also, antitrust sought to preserve open markets, so new enterprises and entrepreneurs could have a fair likelihood of successful entry.[614]

In turn, whilst the origins of Article 102 TFEU are not 'well documented',[615] there is consensus that the policy underpinning Article 102 TFUE was inspired by the ordoliberal school of thought.[616] Ordoliberalism was created in the 1930s by a small group of German economists and lawyers belonging to the 'Freiburg School', who argued that a competitive economic system was required to ensure a prosperous, free and equitable society.[617] Holding the belief that the lack of an effective and reliable legal framework had led to the

---

[608] ibid 737–738.
[609] ibid 738.
[610] According to Justice Peckham, not only are interferences with the competitive process harmful for efficiency reasons, but also given that the "corporate aggrandizement" of trust and combinations is "against the public interest", even if it generates cost reductions that lower price, because "it is in the power of the combination to raise price and the trust may drive out of business the small dealers and worthy men whose lives have been spent in that line of commerce". Justice Peckham, quoted in Jonathan Baker, 'A Preface to post-Chicago Antitrust', in Antonio Cucinota, Roberto Pardolesi, Roger Van den Bergh (eds), *Post-Chicago Developments in Antitrust Law* (Edward Elgar, 2002) 61.
[611] Eleanor M Fox, 'Against Goals' (2012) 81 Fordham L. Rev. 2157, 2158.
[612] Khan (n 604) 739–740.
[613] Robert Pitofsky, 'The Political Content of Antitrust' (1978) 127 U. Pa. L. Rev. 1051.
[614] Khan (n 604) 741.
[615] O'Donoghue and Padilla (n 255) 8.
[616] Liza Lovdahl Gormsen, *A Principled Approach to Abuse of Dominance in European Competition Law* (CUP, 2010) chapter 2; Ian Rose and Cynthia Nqwe, 'The Ordoliberal Tradition in the European Union, Its Influence on Article 82 EC and the IBA's Comments on the Article 82 EC Discussion Paper' (2007) 3 Competition L. Int'l 8, 8; '[T]he prevailing normative understanding of "abuse" may still be said to reflect ordoliberal ideas which have accompanied the drafting as well as the interpretation and application of EU competition law from the very beginning up to the present.' Peter Behrens, 'The Ordoliberal Concept of'Abuse'of a Dominant Position and Its Impact on Article 102 TFEU', *Nihoul/Takahashi, Abuse Regulation in Competition Law, Proceedings of the 10th ASCOLA Conference Tokyo* (2015) 1.
[617] David J Gerber, Law and Competition in the Twentieth Century Europe: (Clarendon Press Oxford, 1998); Rose and Nqwe (n 617) 8.

collaboration between the Nazi government and private cartels as vehicles of totalitarian control and to the economic and political disintegration of Germany, they contended that a legal system had to be established to prevent the creation and misuse of private economic power.[618] Specifically, they held that social welfare could be only achieved through an economic order based on competition, within which the law was in charge of creating and preserving the conditions under which competition could operate properly.[619] Ordoliberals developed the idea of the 'social market economy' (*Soziale Marktwirtschaft*), where individual economic freedom and competition were sources of political freedom, and the economic constitution of society. For ordoliberals, the 'aim of competition policy was limitation and control of private power, or at least of its harmful effects, in order to protect individual economic freedom in the interest of a free and fair political and social order.'[620] Also, they were advocates of open access to the market, as they thought that this was the best control of both private and political power.[621]

It transpires from the above that the competition laws of the US and the EU were informed by considerations other than consumer welfare and economic efficiency. They both shared a concern for the growth of large firms and undue concentrations of economic and political power, a focus on the process of competition instead of its outcome, and the need to keep markets open to avoid abuses and ensure freedom to compete. By focusing antitrust exclusively on consumer welfare, these values and goals have been relegated to history books. This is an utterly negative state of affairs. As Pitofsky observes: '[i]t is bad history, bad policy, and bad law to exclude certain political values in interpreting the antitrust laws.'[622]

Currently, there is tremendous concentration of wealth and market power in data-driven sectors, and barriers to entry are unassailable. Crucially, the undue concentration of market power in digital advertising and information distribution has resulted in undue political influence. The rising fortunes of Google and Facebook are the flipside of the decline of traditional news businesses.[623] Whilst news outlets are forced to reduce their budgets and therefore the quality and amount of news content, the vacated space for news is filled with content that Facebook's and Google's algorithms deem to be the most relevant, regardless of its authenticity, origin or potential detrimental effects, leading to polarisation and disinformation in political culture in an effort to sale targeted ads.[624] One of the recent unintended consequences of this *process* has been the misuse of Facebook's political power

---

[618] O'Donoghue and Padilla (n 255) 8–9.
[619] ibid 9.
[620] Liza Lovdahl Gormsen, *A Principled Approach to Abuse of Dominance in European Competition Law* (Cambridge University Press 2010) 42.
[621] ibid.
[622] He continues: 'By "political values," I mean, first, a fear that excessive concentration of economic power will breed antidemocratic political pressures, and second, a desire to enhance individual and business freedom by reducing the range within which private discretion by a few in the economic sphere controls the welfare of all. A third and overriding political concern is that if the free-market sector of the economy is allowed to develop under antitrust rules that are blind to all but economic concerns, the likely result will be an economy so dominated by a few corporate giants that it will be impossible for the state not to play a more intrusive role in economic affairs.' Pitofsky (n 614) 1051.
[623] Ghosh and Scott (n 29) 50.
[624] Ghosh and Scott argue that although Facebook and other online platforms 'cannot be considered news editors in the traditional sense, they do perform one key editing task: selecting which content their audience will see. In so doing, they choose not to select content based on a set of judgements related to the democratic role of public service journalism (i.e. out of a principled commitment to inform the public). Instead, they make selections based on what will keep the user on the platform longer, thus enabling the display of more ads and the collection of more user data.' ibid 38.

and concomitant interference with democratic processes by ill-intended actors. In order to honour the legislative intent and informing values and goals of the US and EU competition laws, an approach to competition policy 'that focuses on the neutrality of the competitive process and the openness of market structures'[625] is required.

Indeed, this approach is significantly more suitable to assess competition in data-driven sectors, as the Chicago School's focus on outcome (i.e. whether prices rise) has proved incapable of preventing concentration and the exploitation of consumers. As Khan explains, the Chicago School's approach 'presumes that market power is benign *unless* it leads to higher prices or reduced output —[…] glossing over questions about the competitive process in favor of narrow calculations. In other words, this approach equates harm entirely with whether a firm *chooses* to exercise its market power through price-based levers, while disregarding whether a firm has *developed* this power, distorting the competitive process in some other way.'[626] The application of this approach to Facebook's exploitative abuse explained in Section III.A would lead to the conclusion that no market power has been abused and therefore no harm to consumers has ensued, disregarding the fact that Facebook resorted to data privacy violations and deception to amass market power and be ultimately able to impose unfair trading terms on consumers, thereby degrading service quality and impairing consumer choice. To promote competition, Khan proposes an approach that contemplates the assessment of a number of factors that shed light on the state of the competitive process and the openness of markets, including entry barriers, conflicts of interest, the emergence of gatekeepers or bottlenecks, the use of and control over data, and the dynamics of bargaining power.[627] In light of the zero prices and the role and significance of data that characterise data-driven markets, attention to the structural factors above and the adoption of a 'protection of the competitive process' standard, as put forward by Wu,[628] are proposals that competition enforcers should follow.

---

[625] Khan (n 604) 744.

[626] ibid 744–745.

[627] ibid 746.

[628] Wu argues: '[T]he leading alternative standard, the "protection of competition", is at least as predictable, and arguably more determinate than the exceeding abstract consumer welfare test, while being much truer to the legislative intent underlying the antitrust laws. More concretely, we should return to asking, in most antitrust cases, the following question: Given a suspect conduct (or merger): Is this merely part of the competitive process, or is it meant to "suppress or even destroy competition?" This standard actually already forms a part of antitrust doctrine. What changes is eliminating "consumer welfare" as a final or necessary consideration in every case. Here is why the protection standard might be more practical than consumer welfare was. There is a fundamental and important difference between a law that seeks to maximize some value, and one that is designed to protect a process. The maximization of a value, particularly one as abstract as "welfare," necessarily puts enforcers and the judiciary in a challenging position, given that welfare is abstract and ultimately unmeasurable. In contrast, the protection of competition standard puts the antitrust law in the position of protecting the competitive process, as opposed to trying to achieve welfare outcomes that judges and enforcers are ill-equipped to measure. In that sense, it makes the antitrust law akin to the "rules of the game," and make enforcers and judges referees, calling out fouls and penalties, with the goal of ultimately improving the state of play, by protecting a competitive process that actually rewards firms with better products. Beside this practical benefit, as a policy matter, this relatively small change would do much to give antitrust room to achieve its historic goals, and generally make antitrust far more attentive to dynamic harms." 'Tim Wu, 'After Consumer Welfare, Now What? The "Protection of Competition" Standard in Practice' [2018] CPI Antitrust Chronicle.

D. Improvements to Merger Control

Since 2007, Facebook has reportedly acquired 69 companies.[629] This acquisition spree is also seen in other platform giants such as Google, Amazon, Apple and Microsoft.[630]

This trend is problematic. Some of Facebook's acquisitions, especially the acquisitions of Instagram and WhatsApp, undoubtedly increased Facebook's data-driven market power.[631] At the same time, they were the implementation of a 'kill in the crib' strategy, whereby a dominant player buys up nascent or potential competitors having a good potential to displace the incumbent in the future, thereby effectively eliminating a potential competitive threat and reducing competitive pressure.

Importantly, the acquisition strategy of dominant platforms in respect of potential competitors is likely to have a direct impact on disruptive innovation.[632] Whilst the prospect of being acquired by a tech giant serves as an important incentive for innovative start-ups to enter the market, this prospect is double-edged. Indeed, '[i]f innovators and their investors have learned that the biggest payoff is through creating something that complements the status quo, rather than seeking to disrupt or replace the incumbents, then funding will naturally feed through to this form of research.' [633]

Merger under enforcement in digital markets can be attributed to the jurisdictional thresholds that trigger merger review in the EU, the US and other jurisdictions such as the UK and Germany, and to the narrow consumer welfare standard that is used to assess the likely effects of the merger on competition and consumers.

In the EU, the jurisdictional thresholds that determine whether a concentration will be assessed by the Commission or a national competition authority (NCA) such as the CMA are defined in terms of the turnovers of the acquiring and target undertakings. These thresholds were defined to establish a convenient system to allocate jurisdiction between the Commission and the NCAs of Member States, at a time when revenues were generated mostly from contracts with customers. However, they are unsuitable to data-driven markets where value is represented by the user base of a service or the number of visitors to a website. For example, Facebook paid substantial amounts of money to acquire WhatsApp and Instagram, but since the targets were hardly making any profits, the concentrations did not meet the thresholds that establish an EU dimension and trigger the obligation to notify the concentration to the Commission. Inadequate turnover-based thresholds 'may well have contributed to hundreds if not thousands of tech sector mergers being completed "under the radar" and to increased levels in the concentration of the sector over time.'[634] Commenting on the UK context, Furman *et al.* observe that there were approximately 250 acquisitions in the last 5 years, and none of these mergers were

[629] 'Facebook - Acquisitions' (*Crunchbase*) <https://www.crunchbase.com/organization/facebook/acquisitions/acquisitions_list>.
[630] In the last decade, Amazon, Apple, Facebook, Google, and Microsoft combined have made over 400 acquisitions globally. Some of these acquisitions have been of exceptionally high value, peaking with Microsoft paying USD26.2 billion for LinkedIn. Jason Furman and others, 'Unlocking Digital Competition. Report of the Digital Competition Expert Panel' (2019) 91.
[631] As a result of data-driven externalities. See Section I.C.2.
[632] Furman and others (n 631) 48.
[633] ibid 50.
[634] Tim Cowen and Phillip Blond, '"TECHNOPOLY" and What to Do about It: Reform, Redress and Regulation' (2018) ResPublica 24.

voluntarily notified to the CMA.[635] Accordingly, to capture these mergers, alternative notification thresholds should be included in the EUMR and the merger control laws of other jurisdictions, such as thresholds based on the size (value) of the transaction, the user base (number of users) of the merging firms, or the value of data involved in the transaction.

The shortcomings of the consumer welfare standard were explored in the preceding section. This standard must be broadened to encompass non-price facets on competition, especially innovation. In addition, in the context of merger control, the effects of concentrations on potential competition deserve special attention. As Carl Shapiro argues:

'[o]ne promising way to tighten up on merger enforcement would be to apply tougher standards to mergers that may lessen competition in the future, even if they do not lessen competition right away. In the language of antitrust, these cases involve a loss of potential competition. One common fact pattern that can involve a loss of future competition occurs when a large incumbent firm acquires a highly capable firm operating in an adjacent space. This happens frequently in the technology sector. Prominent examples include Google's acquisition of YouTube in 2006 and DoubleClick in 2007, Facebook's acquisition of Instagram in 2012 and of the virtual reality firm Oculus VR in 2014, and Microsoft's acquisition of LinkedIn in 2016.'[636]

The problem with the loss of future competition and harm to innovation is that they are highly uncertain at the time of the merger. Therefore, proving that a significant impediment to effective competition or a substantial lessening of competition is more likely than not can be impossible, despite the potential detrimental effects of the merger. Accordingly, a 'balance of harms' approach could be applied to digital mergers, which would entail that mergers are blocked when they are expected to do more harm than good.[637] Taking the example of the *Facebook/Instagram* merger, Furman *et al.* explain:

'a balance of harms approach would consider the potential harm from losing a powerful rival to Facebook's social network. This harm would include the forgone benefits from the competition that a rival could bring, for example through increased quality and availability of innovative new services, lower costs of digital advertising being passed through to consumers, and greater privacy protection. Importantly, the scale of these potential impacts would be factored into the decision to a greater extent than is possible under the current test.'[638]

Last but not least, merger control should be particularly wary of vertical and conglomerate mergers that lead to concentrations of datasets giving rise to a competitive advantage in multiple data-driven segments. For example, in the *Facebook/WhatsApp* merger the combination of data post-transaction is almost certain to have entrenched Facebook's position in the market for social networking services. Indeed, since August 2016 the phone numbers of WhatsApp users began to be shared with Facebook, which enabled the latter to run analytics on user activity and make friends suggestions based on people with whom

[635] Furman and others (n 631) 91.
[636] Carl Shapiro, 'Antitrust in a Time of Populism' (2018) 61 International Journal of Industrial Organization 714, 739–740.
[637] Furman and others (n 631) 99.
[638] ibid.

users talk on WhatsApp.[639] This effect was painfully absent in the Commission's assessment.

V. CONCLUSIONS

The purpose of this paper was to explore whether Facebook's violations of data protection law, privacy law and consumer law amounted to an abuse of a dominant position under Article 102 TFEU. It concludes that Facebook is violating Article 102 TFEU. Its infringement of Article 102 TFEU is not only due to its violation of the mentioned laws, but because of its actual anticompetitive effects on competition. Facebook pursue, relentlessly and without exception, its own self-interest, regardless of the often harmful consequences it may cause to the users of its platform. Its business model relies on the harvesting and processing of personal data not only from the users of its platform, but also from users of the Internet in general. As a result is has accumulated a near monopoly position in the market and wields it power over people and societies. Within the social space we are inescapably surrounded by Facebook, Instagram, WhatsApp and Messenger apps.

In 1933, Supreme Court Justice Louise Brandeis likened powerful corporations to evil 'Frankenstein monsters'.[640] According to Brandeis, the regulatory system was designed to control and prevent powerful corporations from causing harm. Regrettably, more than 80 years later we are in a situation where Facebook has accumulated so much power, it can fully exploit its users, app developers, publishers and advertisers and exclude any potential competitors seemingly without any regulatory consequences. While policymakers and regulators across the globe grapple with what to do with Facebook, Facebook continues to distort competition on a massive scale.

Facebook has again and again shown it is unable to be socially and legally responsible. Perhaps it is too much to ask of a for-profit corporation. It is after all the job of regulators to protect citizens from corporate misdeeds in form of anticompetitive conduct and promote the public interest. Some national competition regulators notably in Germany and France are actively trying their best, but the Commission is certainly not leading the way when it comes to Facebook. This is interesting given its general activity in digital markets. The Commission has certainly been extremely active in enforcing the antitrust rules against Google. Thus, this paper suggest that the Commission take a serious look at Facebook's business model to restore competition in the social network market.

[639] Duran (n 517) In turn, more friends connections translate into more user engagement and therefore more data to train its social network algorithms and enhance further its ad targeting capabilities. .
[640] Louis K. Liggett Co. et al. v. Lee, Comptroller et al., 288 US 517 (1933) 567, 548.