Exploitative Data Harvesting

as an Article 102 TFEU Violation

Submitted for the Degree of:

Master of Philosophy in Law

July 2021

Candidate: **Ambika Vadehra, St Antony's College**

Supervisor: **Professor Ariel Ezrachi**

ABSTRACT

The digital landscape has become an intrinsic part of our day-to-day lives and has brought numerous benefits to society. A key factor which has enabled such digital (and societal) transformation is big data and platforms' enhanced abilities to harvest, analyse and use the same. However, despite the distinct benefits provided by big data and analytics, some harmful implications, including in the competition law sphere are notable. Various aspects of such harm are relevant from an antitrust perspective - this thesis focuses on exploitative data collection by dominant platforms and its privacy-degrading implications.

Notably, there has already been some enforcement action in this area against Facebook's data collection practices by the German competition authority; and more recently, Germany also started investigating Google's data processing terms. Similarly, Facebook's privacy-degrading data gathering practices were also highlighted in recent complaints (by the FTC and State Attorney Generals) in the US.

These cases raise interesting questions for EU competition; specifically, can dominant platforms' exploitative data harvesting practices be sanctioned under Article 102 TFEU as an abuse of dominance?

The thesis explores this issue. After discussing big data and dominant platforms' exploitative data collection practices, it establishes the intersection of privacy and antitrust in this sphere. Then it discusses how despite traditional reasons for limited enforcement appetite in exploitative abuse cases, such intervention is justified in the data economy. Thereafter, it explores two potential theories of harm, and concludes that viewing *privacy-quality*

degradation as an exploitative abuse of dominance is a feasible and practically enforceable approach. Finally, it discusses Article 102 TFEU as part of a wider enforcement toolbox, and the complementary role to be played by other antitrust tools and external legislative frameworks like data protection, consumer laws and platform-specific regulation; where these other tools rectify broader market conditions, and ex-post competition law corrects specific failures.

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

BkM	Bundeskartellamt or German Competition Authority
CJEU	Court of Justice of the European Union
CMA	Competition and Markets Authority
Cremer Report	Competition Policy for the Digital Era (2019), Report by the Directorate-General for Competition (European Commission)
DMA	Digital Markets Act
DMU	Digital Markets Unit
DRCF	Digital Regulatory Cooperation Forum
DSA	Digital Services Act
EC/Commission	European Commission
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
EU P2B Regulation	EU Platform-to-Business Regulation
FCA	Financial Conduct Authority
French-German Report	Competition Law and Data (2016), Report by Autorité de la Concurrence and Bundeskartellamt
FTC	Federal Trade Commission

Furman Report	Unlocking Digital Competition (2019), Report of the Digital Competition Expert Panel (UK)
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IoT	Internet of Things
JFTC	Japan Fair Trade Commission
NCA	National Competition Authority
OfCom	The Office of Communications
PETs	Privacy Enhancing Technologies
SMS	Strategic Market Status
Stigler Report	Stigler Committee on Digital Platforms, Final Report (2019)
TFEU	Treaty on the Functioning of the European Union
ToH	Theory/Theories of Harm
UB	United Brands
UCPD	Unfair Commercial Practices Directive
UCTD	Unfair Contractual Terms Directive
US HJR	United States House Judiciary Report or Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary, Investigation of Competition in Digital Markets (Majority Staff Report and Recommendations, 2020)
WSJ	Wall Street Journal

TABLE OF CASES

EU and Member State Cases

UK Cases

US Cases

TABLE OF STATUTES

Statutes

Guidelines

TABLE OF REPORTS

Reports

INTRODUCTION

> *Data are an essential factor for economic strength, and a decisive criterion in assessing online market power…. [w]henever data are collected and used in an unlawful way, it must be possible to intervene under antitrust law to avoid an abuse of market power*.[1]
> - Andreas Mundt (President, German Competition Authority ('BkM'))

The digital landscape has become an intrinsic part of our day-to-day lives, and has brought numerous benefits to society. It has transformed how we consume information, interact, think, search, shop and relax; and has created new markets and fresh opportunities which were previously unthinkable, such as driverless cars, digital assistants, wearable devices, better analytics for manufacturing etc.[2] And, despite the notorious Zoom fatigue, it is only because of today's online ecosystems that certain aspects of daily life have been able to function somewhat 'normally' in the midst of the Coronavirus pandemic.

A key factor which has enabled such digital (and societal) transformation is big data and platforms' enhanced abilities to harvest, analyse and use the same. However, despite the various benefits provided by the increasing use of big data, some harmful implications across different spheres of law, including competition law, are noticeable. In this context, jurisdictions globally are debating whether data-driven ecosystems require a re-thinking of

[1]Lomas, 'Antitrust case against Facebook's 'super profiling' back on track after German federal court ruling' (*TechCrunch*, 23 June 2020) < https://techcrunch.com/2020/06/23/antitrust-case-against-facebooks-super-profiling-back-on-track-after-german-federal-court-ruling/> accessed 26 May 2021.

[2]Ezrachi and Robertson, 'Competition, market power and third-party tracking' (2019) SSRN 1.

how antitrust law applies to digital markets, for instance in relation to analytical tools and the way that anticompetitive behaviour is understood.[3]

This thesis focuses on one such area of concern – adverse implications of exploitative data collection by dominant platforms and whether such conduct can be sanctioned as an abuse of dominance under EU competition law; an area which until recently, has received relatively sparse attention in the antitrust community.

Notably, such action for exploitative data collection has already been taken by the BkM against Facebook (the German Facebook case)[4], which was confirmed on appeal by Germany's highest court.[5] And although this decision was recently referred to the CJEU[6], the BkM has already initiated a similar investigation into Google; specifically, in respect of Google's data processing terms and to investigate if users will '*have sufficient choice as to how Google will use their data*'.[7] Similarly, competition enforcers across other jurisdictions have also started scrutinizing the antitrust implications of dominant platforms data collection

[3]Robertson, 'Antitrust Law and Digital Markets: A Guide to the European Competition Law Experience in the Digital Economy' (2020) REWI 1< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3631002 > accessed 24 June 2021.

[4]'Bundeskartellamt prohibits Facebook from combining user data from different sources' (*Bundeskartellamt*, 7 February 2019) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html> accessed 4 June 2021.

[5]Knapp and Busvine, 'Top German court reimposes data curbs on Facebook' (*Reuters*, 23 June 2020) <https://www.reuters.com/article/us-facebook-germany-idUSKBN23U2P4> accessed 4 June 2021.

[6]'Dusseldorf Court Asks ECJ To Review Facebook Data Case' (*Competition Policy International*, 24 March 2021) <https://www.competitionpolicyinternational.com/dusseldorf-court-asks-ecj-to-review-facebook-data-case/> accessed 4 June 2021.

[7]'Proceeding against Google based on new rules for large digital players (Section 19a GWB) – Bundeskartellamt examines Google's significance for competition across markets and its data processing terms'(*Bundeskartellamt*, 25 May 2021) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/25_05_2021_Google_19a.html?nn=3591568> accessed 27 May 2021.

practices and consequent user privacy degradations; and as recently noted by Isabelle de Silva (France's competition chief), '*Privacy and competition will be one of the big topics of the year*'.[8]

In light of such developments, this thesis discusses the timely question of whether action similar to the German Facebook case can and should be pursued under EU competition law. Specifically, it explores if the traditional boundaries of Article 102 TFEU can be effectively re-conceptualized through new Theories of Harm (ToH), such that it can be used to sanction platforms' exploitative data harvesting conducts.

The structure of this thesis is as follows:

Section 1 discusses specifics regarding big data and the cycle of data collection, and how platform's practices in this regard can result in significant consumer exploitation, specifically through a degradation of user privacy.

Section 2 focuses on the intersection of big data and competition law, and discusses why antirust intervention is warranted in context of such privacy-reducing conducts by dominant platforms.

Section 3 discusses exploitative abuses under Article 102 TFEU; specifically, its' evolution in traditional markets and historical reasons for limited intervention appetite in this area.

Section 4 explores how the traditional arguments against intervention in exploitative abuse cases don't apply in the data economy. It establishes the rationale for Article 102 TFEU intervention in this sphere and introduces two key ToH for sanctioning exploitative data harvesting.

[8]Scott, 'In battle for privacy, antitrust watchdogs throw their hat in the ring' (*Politico*, 24 May 2021) <https://www.politico.eu/article/battle-privacy-antitrust-watchdogs-throw-their-hat-in-the-ring/> accessed 4 June 2021.

Section 5 discusses the first ToH, i.e., excessive data harvesting as an Article 102 TFEU violation, as part of which it explores three key approaches. Specifically, it looks at: (i) excessive data collection as an excessive pricing abuse (ii) excessiveness and fairness of data collection relative to the service, and (ii) excessiveness in relation to an external benchmark. This Section concludes that although all three approaches under this ToH are theoretically feasible (to varying degrees), their underlying complexities could still deter actual enforcement, thereby creating room for another ToH.

Section 6 discusses the second ToH, i.e., degradation of privacy-quality as an exploitative abuse. It establishes how privacy can be treated as a dimension of product quality (an important competitive parameter), and an unjustified reduction of such privacy-quality can be regarded as exploitative, similar to how excessive prices can be exploitative. Accordingly, it puts forward a ToH which provides a direct link between privacy and consumer welfare (through the quality parameter), and briefly highlights suitable remedies.

Section 7 considers Article 102 TFEU as part of a wider toolbox, and establishes the complementary role to be played by other instruments in curtailing exploitative data harvesting. Specifically, it looks at other antitrust tools (merger control and market investigations); and non-antitrust tools like data protection, consumer enforcement and platform specific ex-ante regulation.

This is followed by the Conclusion.

1. BIG DATA AND THE CYCLE OF DATA COLLECTION

> *Personal Data is the new oil of the internet and the new currency of the digital world.*
>
> - Meglena Kuneva, former Consumer Protection Commissioner (Speech at the Roundtable of Online Data Collection, Targeting and Profiling, Speech 09/156).

This observation, made in 2009, has proved to be increasingly prescient with time. Today the digital economy is a central part of our lives; and at its' heart, lies big data. Everything we see around us – from online search and social media to Amazon's Alexa and the NHS track-and-trace app – is fueled by big data and big analytics. And with big data increasingly playing a pivotal role in companies' strategic decision-making and business models, this trend will only intensify over time, ultimately leading to an '*Internet of Everything*'.[9] Despite its numerous benefits however, big data can have significant harmful implications for the society and economy, including at the stage when it is collected from users – the key focus of this thesis.

Before delving into specific antitrust provisions and ToH for sanctioning dominant platforms' exploitative data harvesting; this first Section explores big data and the mechanics of data collection and use, and provides essential context to such discussion. Part 1.1 discusses big data – specifically its centrality in today's economy and the competitive significance thereof. Part 1.2 elaborates on the mechanics of firms' data harvesting practices and how these

[9]Cisco, 'The Internet of Everything' (IoE Value Index Study, 2013) <https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf> accessed 26 May 2021.

have resulted in data bottlenecks. Part 1.3 discusses harmful implications, specifically consumer exploitation and manipulation, arising from such widespread tracking orchestrated by a few dominant players.

1.1 BIG DATA

Big Data- A crucial engine

'Big Data' is broadly understood as large amounts of different types of data produced at a high speed from multiple sources, with increasing socio-economic value; and, is characterized by the four V's –Volume, Velocity, Variety, and Value.[10]

An extensive *Volume* of data is collected on individuals on a daily basis, for instance due to the increasing migration of social and economic activities to the Internet, the decreasing cost of collecting and processing data, the rise of broadband access/smartphones/Internet of Things (IoT) etc.[11] Big data also entails that data is being generated, collected and analysed at an increased speed or *Velocity*; as illustrated by nowcasting i.e., using data and predicting what is happening in real-time, a prevalent practice in predicting flu rates, real estate trends, traffic conditions, health metrics etc.[12] Similarly, big data is characterized by a *Variety* of data being collected on individuals, example by integrating data from multiple sources; and the *Value* of data, which is reinforced by the other three Vs and the quality of data analytics (i.e.,

[10]Autorité de la concurrence and Bundeskartellamt, *Competition Law and Data* (2016) 4 (French-German Report).

[11]Stucke & Grunes, *Big Data and Competition Policy* (1st edn, OUP 2016) 16.

[12]ibid at 19, 20.

the technical means to extract insights from, analyse and speedily act upon data).[13] Notably, there has been a rapid increase in each *V* over the past decade, made possible through significant technological advancements in computing and processing power, network connections, cloud-based systems and powerful algorithms.[14]

Although the term 'big data' is often used in varying contexts, one of its underlying features is its centrality to the digital landscape - so much so, that it is '*self-evident that data is key to digital platforms'* (Valletti).[15] Another key feature of big data is its heterogeneity. Specifically, it can broadly be categorized according to, (i) type of information provided i.e., non-personal or personal data; (ii) use i.e., individual-level (anonymous/non-anonymous), aggregated or contextual data; (iii) structured, unstructured or semi-structured data; (iv) means of acquisition – volunteered, inferred, observed or purchased/licensed data etc.[16]

This thesis focuses on personal data, which is generally defined as '*any information relating to an identified or identifiable individual (data subject)*'.[17] The collection and use of personal data have enabled the provision of many new types of services and resulted in the prevalence of data-driven business models. This includes multi-sided platforms providing targeted advertisements along with (ostensibly) free services, example music and video

[13]ibid at 21.

[14]French-German Report (n 10) 8.

[15]Data and Privacy Hearing, 'Testimony of Tommaso Valletti, Professor of Economics, Imperial College Business School' (*House Judiciary Committee - Subcommittee on Antitrust, Commercial, and Administrative Law*, 18 October 2019) 2 <https://www.congress.gov/116/meeting/house/110098/witnesses/HHRG-116-JU05-Wstate-VallettiT-20191018.pdf> accessed 26 May 2021.

[16]Directorate-General for Competition (European Commission), *Competition Policy for the Digital Era* (2019) 24-26 (Cremer Report).

[17]General Data Protect Regulation (GDPR), Article 4(1); OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* (OECD Digital Economy Paper No 220, 2013) 7

streaming, online search, social networking etc.; provision of individualized services like match-making, personalized search and recommendations; individualized pricing, example price steering, price discrimination; and, onwards data sales or data brokerage.[18] It has also enhanced the quality of goods/services and enabled the exploitation of new business opportunities.[19] As such, personal data is a crucial asset which can help deliver efficiencies and value for platforms, sellers, advertisers, content providers and consumers.[20]

Importantly, personal data doesn't just enable such target-oriented business models, but is also crucial to them. For instance, the average (online) publisher revenue from users drops by almost 52% in the absence of specific targeting based on behavioral consumer data.[21] Therefore in today's economy, data plays a critical role in how digital platforms compete, as further discussed below.

The competitive significance of data

There has been some debate about the competitive significance of data. It is sometimes argued that data has certain economic characteristics, i.e., it is ubiquitous, low cost, widely available, non-rivalrous, non-exclusive, and easily collected and replicated; due to which any benefits

[18]Ezrachi and Robertson (n 2) 2,3.

[19]Report of the Digital Competition Expert Panel (UK), *Unlocking Digital Competition* (2019) para 1.40 (Furman Report).

[20]Ezrachi and Robertson (n 2) 1.

[21]Srinivasan, 'The intersection of privacy, data and competition' (*Promarket,* 26 October 2019) <https://promarket.org/2019/10/26/the-erosion-of-privacy-for-facebook-and-google-users-is-an-antitrust-problem/> accessed 26 May 2021.

provided by data can be easily duplicated, and its accumulation by itself doesn't lead to a competitive advantage.[22]

However, this claim ignores the key role played by the accessibility and substitutability of data, and how in the real world these are often severely constrained through means like technical restrictions and legal contracts.[23] Therefore, the non-rivalrous characteristic of data does not diminish its significance as in practice, firms can (and do) restrict competitors' access to the same. Additionally, big data displays positive feedback loops i.e., control over some of an individual's data, and its aggregation, increase the platform's ability to collect more of it and improve its targeting.[24] This self-reinforcing data advantage combined with the winner-takes-all economics of digital markets (due to network effects, switching costs, lock-in and increasing returns to scale and scope) further reinforces the competitive significance of data; which constitutes a substantial source of market power and often acts as a barrier to entry.[25]

Consequently, a data advantage can create dominant (and even, super-dominant) positions of power and enable firms to expand and sustain their monopoly position. As noted in the US House Judiciary Report (US HJR):

[22]Sokol and Comerford, 'Does antitrust have a role to play in regulating big data?' in Blair and Sokol (eds), *The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech* (CUP 2017) 6.

[23]Stucke and Grunes (n 11) 7-9.

[24]Cremer Report (n 16) 31.

[25]Stigler Committee on Digital Platforms, *Final Report* (2019) 7 (Stigler Report).

> *Data allows companies to target advertising with scalpel-like precision, improve services and products through a better understanding of user engagement and preferences, and more quickly identify and exploit new business opportunities.*[26]

Additionally, big data's competitive significance has also led to the emergence of 'data-opolies' i.e., data-rich companies controlling a key platform which in turn attracts users, sellers, advertisers, apps etc., to its ecosystem; example, Facebook, Google, Amazon and Apple.[27]

Given its market power implications and scope for monetization, firms are incentivized to collect and use as much personal data as possible. Rapid advancements in technology in conjunction with lack of consumer awareness and regulatory intervention in this sphere enables them to do so. However, digital platforms' data collection practices are far from unproblematic, and '*[w]henever data are collected and used in an unlawful way, it must be possible to intervene under antitrust law to avoid an abuse of market power*' (Mundt).[28]

The thesis will focus on this stage of data acquisition by dominant firms and explore whether European competition law, specifically Article 102 TFEU, can target such practices. Now, let's discuss the mechanics of data collection (Part 1.2) and the harmful implications thereof (Part 1.3).

[26]Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary, *Investigation of Competition in Digital Markets* (Majority Staff Report and Recommendations, 2020) 42 (US HJR).

[27]Stucke, 'Should we be concerned about Data-opolies?' (2018) 2 Georgetown Law Technology Review 275.

[28]Lomas (n 1).

1.2 HOW IS DATA OBTAINED?

Tracking

Today most of our activities, online *and* offline, leave a digital trace and individual data can be collected from a wide variety of sources using tracking technologies. These include 'cookies' (traditionally used on web browsers) and tracking pixels (similar to cookies, but more useful in context of smart phones); consumer identifying characteristics like log-ins (deterministic methods); IP addresses, geolocation information, browser or device fingerprinting, general usage patterns etc., to infer consumer identity (probabilistic methods).[29] These technologies enable firms to track web users within and across pages on the internet, and across devices like laptops/smartphones/voice-assistants etc. For instance, of 100 popular websites used across two devices, at least 87 used cross-device tracking, 96 allowed consumers to submit a username or email address, and 16 shared user names or emails with third parties.[30]

These tracking technologies can be used to collect both 'first-party' and 'third-party' data.[31] When data is collected by a firm in the course of its' relationship with the customer, it is first-party data; example, Google collecting data from Google search/Gmail users. In contrast, data used by specific platforms but collected by another entity is referred to as third-party data; ex., Google's collection of user data on non-Google websites and apps. Depending on whether data is collected with or without proper user knowledge/consent, data harvesting

[29]Federal Trade Commission, *Cross-Device Tracking* (FTC Staff Report, 2017) 2.

[30]ibid 4.

[31]OECD, *Consumer Data Rights and Competition - Background note* (DAF/COMP (2020)1) 16 (OECD Data-Rights Report).

can be either authorized or unauthorized; and from this perspective, data collection through third-party tracking often tends to be more problematic.

Third-party tracking

Third-party tracking allows a tracker to harvest extensive amounts of personal user data from a variety of sources, actively and passively, thereby allowing it to create large datasets. Here, the first-party website embeds content from a third-party, and since the same third-party code is often embedded on different (first-party) websites or apps, a single user's behavior on multiple different apps/websites can be tracked by the third-party.[32] The information gathered includes users' interests, demographics, content viewed, geolocation data, items purchased/browsed, personal communications etc.[33] This data can then be combined to build comprehensive behavioral user profiles, which in about 75% cases allows the individual to be identified[34]; consequently enabling a world of '*targeted everything*'[35].

Significant tracking occurs both on the web and across applications. For instance, over 90% (of a million) free mobile phone apps have a third-party tracker, and some (nearly 18%) over twenty different trackers.[36] Similarly, 95% of the world's top websites have at least one

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

[33]Binns et al., 'Measuring third party tracker power across web and mobile' (2018) arXiv:1802.02507 3, 9; Binns et al., 'Third party tracking in the mobile ecosystem' (2018) ACM WebSci'18, 1.

[34]Robertson, 'Excessive data collection: Privacy considerations and abuse of dominance in the era of big data' (2020) 57(1) Common Market Law Review 161, 163. *See also* Krishnamurthy, Naryshkin and Wills, 'Privacy Leakage vs. Protection Measures: The Growing Disconnect' (2011) Proceedings of the Web 2.0 Security and Privacy Workshop 5.

[35]Ezrachi and Robertson (n 2) 1.

[36]ibid 3.

third-party tracker, and 70% have more than one.[37] Some third parties (like LiveRamp) also specialize in matching online users to their offline profiles held by data brokers.[38]

Many third-party trackers have legitimate uses, including providing basic measurements for the first-party (ex., how an app is used), functionalities (ex., authentication, bot-blocking) etc. However, one of the key functions of such tracking is profiling of users for targeted advertising and extracting insights from their behavior for analytics, which firms monetize extensively. And importantly, this tracking capability is predominantly concentrated in the hands of few dominant players, creating bottlenecks.

Bottlenecks in data collection

In a telling metaphor the third-party tracking ecosystem has been compared to a tree, where trackers are like its widespread branches, and companies owning these trackers are like the roots of the tree with a very limited spread.[39] As such, certain companies represent power junctions at which data harvested through third-party tracking converges; namely, Alphabet/Google (present on 90% of top domains and 88.44% of all apps), followed by Facebook, Microsoft and Twitter.[40]

In conjunction with the third-party tracking mechanism, dominant platforms also often use their dominance and integration across other markets to increase touchpoints for mining

[37]Purra and Carlsson, 'Third-Party Tracking on the Web: A Swedish Perspective' (IEEE 41st Conference on Local Computer Networks (LCN), 2016) 28, 31.

[38]Binns and Bietti, 'Dissolving Privacy, One Merger at a Time: Competition, Data and Third-Party Tracking' (2020) 36 Computer Law & Security Review 6.

[39]Ezrachi and Robertson (n 2) 3.

[40]ibid.

user data. For instance, Google has leveraged its' ownership of Android to ensure that smartphones enhance Google's data collection efforts and '*to extensively surveil its users*'.[41] Example, through client ID configuration - a unique alphanumeric code incorporated in the smartphone - Google can combine metrics tracked via the hardware with all the other data Google collects on users. Similarly, Facebook's acquisition of Giphy implies being tracked by Facebook while sending GIFs online, even if users have otherwise blocked Facebook ad pixels or deleted their Facebook accounts.[42] Dominant firms can also use '*privacy policy tying*' envelopment strategies to obtain broad consumer consent from its users across markets, which increases the amount of data they can collect across platforms.[43] Businesses are also increasingly using customer loyalty schemes to harvest consumer data.[44] Additionally, with the rise in IoTs, which have a significant grey area surrounding user consent, such covert techniques and unauthorized data harvesting will only increase. Reportedly, Amazon made Vivint's (a manufacturer of smart-home devices) continued presence on Echo conditional on Vivint providing Amazon with data from every Vivint device in customers' homes at all times (and not just data from Vivint's function on Echo*).*[45]

[41]US HJR (n 26) 217.

[42]Williams, 'How Facebook Could Use Giphy to Collect Your Data' (*Onezero,* 15 May 2020) <https://onezero.medium.com/how-facebook-could-use-giphy-to-collect-your-data-70824aa2647b> accessed 26 May 2021.

[43]Condorelli and Padilla, 'Harnessing Platform Envelopment in the Digital World' (2020) 16(2) Journal of Competition Law & Economics 143.

[44]OECD Data-Rights Report (n 31) 16.

[45]Mattioli and Lombardo, 'Amazon Met With Startups About Investing, Then Launched Competing Products' (*The Wall Street Journal* (WSJ), 23 July 2020*)* <https://www.wsj.com/articles/amazon-tech-startup-echo-bezos-alexa-investment-fund-11595520249> accessed 26 May 2021.

Notably, such extensive data harvesting by a few dominant companies not only enhances their data advantage and market power, but also enables them to exploit consumers and cause a real sense of distortion.

1.3 IMPLICATIONS - CONSUMER EXPLOITATION

> *The desire to put profits over privacy is nothing new…..[t]hese scraps of data, each one harmless enough on its own, are carefully assembled, synthesised, traded and sold. … This is surveillance. These stockpiles of personal data serve only to enrich the companies that collect them. This should make us very uncomfortable. It should unsettle us.*[46]
>
> - Tim Cook

Dominant platforms have increasing monetary incentive and abilities to collect as much user data as possible; however, as noted in the quote above, such conduct can have significant exploitative implications. Notably, the market for data is characterized by substantial asymmetries of information and lack of transparency, with most users in the dark about how much information is being collected about them, sold and used to make a profit.[47] This is broadly because platforms' widespread data harvesting techniques though ubiquitous, are often covert; and although consumers often do volunteer their information online, '*the volume of information that people create themselves…..pales in comparison to the amount of digital information created about them each day*'.[48] For instance, not many individuals are aware that some popular Android apps collect their location information on an average of once every

[46]Cook, 'Keynote Address' (40th International Conference on Data Protection and Privacy, Brussels, 24 October 2018) <https://www.youtube.com/watch?v=kVhOLkIs20A> accessed 26 May 2021.

[47]Stigler Report (n 25) 53.

[48]Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (2014) 2 <https://w ww.whitehouse.gov/sites/default/fi les/docs/big_data_privacy_ report_may_1_ 2014.pdf> accessed 26 May 2021.

three minutes.[49] As such, there is a significant degree of user exploitation and manipulation involved in *how* platforms acquire user data.

For instance, platforms are increasingly using manipulative design interfaces like framing, nudges, default options, and other dark patterns i.e., interfaces that make it difficult for users to express or act according to their actual preferences.[50] Such techniques are exploitative as they are deliberately designed to exacerbate information asymmetries and leverage on users' well-established biases and heuristics (ex., by increasing consumer's search/evaluation costs), to enhance firms' market power and '*maximize a company's ability to extract revenue from its users'*.[51] Notably, such practices are pervasive in the privacy and security sphere. For instance, a simple manipulation of user interfaces (ex., highlighting or hiding specific buttons) can increase acceptance rates of a data protection plan by 228% without companies facing significant consumer backlash.[52] As platforms continue to increase investments to extract excessive amounts of data, such manipulative interfaces will only get more sophisticated in the future.

Platforms also funnel users within their ecosystems using other covert mechanisms like search engine manipulation/bias, ranking biases, filtering and ordering search suggestions etc.; which can limit the visibility/availability of outside options to consumers and ensure that they remain on the platform. Example, Google routinely uses its search dominance to

[49]Dwoskin, 'Apps Track Users—Once Every 3 Minutes' (*WSJ*, 23 March 2015) < https://www.wsj.com/articles/apps-track-usersonce-every-3-minutes-1427166955> accessed 26 May 2021.

[50]Calo, 'Digital Market Manipulation' (2014) 82(4) The George Washington Law Review 995; CMA, *Online Platforms and Digital Advertising* (Market Study Final Report, 2020) 14; Stigler Report (n 25) 237.

[51]US HJR (n 26) 53.

[52]Stigler Report (n 25) 12, 211, 246.

prioritize its own content on the search results page, which ensures that users would remain '*within its walled garden indefinitely'*.[53] By increasing user search/switching costs and lock-in, such techniques enable platforms to intensify the amount of data they collect from users and to exacerbate user vulnerability to behavioral techniques and control by the platform. Additionally, such conducts also enable other forms of user exploitation like price and behavioural discrimination, manipulation of news feeds/search results, micro-targeting etc.; and, also have an exclusionary element (ex., self-preferencing). Notably, such exploitative and exclusionary elements often reinforce each other.

Given their widespread and covert nature, such manipulative tactics and tracking are largely unavoidable; for instance, Facebook's extensive tracking using like-buttons and login-interfaces even if the user is not using these services or has actively objected to web tracking.[54] Additionally, platforms often exhibit blatant disregard for user preferences and data protection rules. Example, Google allegedly harvests user data in Incognito mode and without obtaining user consent[55]; and had also covertly bypassed Safari's blocking of third-party cookies to collect data in breach of user privacy.[56] Similarly, Facebook has also overridden users' privacy settings to transfer data to app developers for its own economic advantage.[57]

[53]US HJR (n 26) 185.

[54]Volmar and Helmdach, 'Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation' (2018) 14(2-3) European Competition Journal 195, 200.

[55]Osborne, 'Google fails to quash Incognito mode user tracking, privacy lawsuit' (*ZDNet* , 15 March 2021) < https://www.zdnet.com/article/google-fails-to-quash-incognito-mode-user-tracking-privacy-violation-lawsuit/> accessed 26 May 2021.

[56]Henderson and Askew, 'Case Preview: Lloyd v Google LLC' (*UK Supreme Court Blog*, 28 April 2021) <http://ukscblog.com/case-preview-lloyd-v-google-llc/> accessed 26 May 2021.

[57]Furman Report (n 19) para 1.125.

Although manipulations are also common in brick-and-mortar shops, digital market manipulation is particularly exploitative of consumers. Online platforms hold a significant amount of varied data on individuals, often from multiple sources, which they can utilize to target and manipulate individual preferences at a scale that goes far beyond what is possible in traditional markets. Delacroix and Veale have noted how this situation essentially creates an epistemic imbalance i.e., a situation where '*a powerful entity knows or understands something concerning an individual that they themselves do not*'; which is then used by platforms to engage in such pervasive profiling, that it can be equated to a form of social cruelty.[58] Additionally, by using detailed, personalized, minute-by-minute control over their interface, online platforms can also often create a façade of competition, choice, and autonomy, whilst simultaneously directing users with behavioural techniques; similar to the Truman Show (Ezrachi and Stucke).[59]

Therefore, there is a clear asymmetry of information and analytical capabilities between users and dominant digital platforms; which often translates into an asymmetry of power, and creates multiple avenues for consumer exploitation. And by engaging in such data collection tactics, dominant firms can significantly undermine consumer privacy and well-being, the democratic process, consumer choice and decision-making sovereignty.[60]

[58]Delacroix and Veale, 'Smart Technologies and Our Sense of Self: Going Beyond Epistemic Counter-Profiling' in Hildebrandt and O'Hara (eds), *Life and the Law in the Era of Data-Driven Agency* (Edward Elgar 2020) 3.

[59]Ezrachi and Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016).

[60]Ezrachi and Stucke, 'Digitalisation and its impact on innovation' (2020) European Commission Working Paper 60; Kuenzler, 'Direct Consumer Influence—The Missing Strategy to Integrate Data Privacy Preferences into the Market' (2020) 39 Yearbook of European Law 423; Podszun, 'Digital ecosystems, decision-making, competition and consumers – On the value of autonomy for competition' (2019) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3420692> accessed 1 July 2021.

This thesis focuses specifically on the privacy-reducing aspect of consumer exploitation caused by dominant platforms' data collection practices; an important area given privacy's significance as a value in itself (especially as a fundamental right in the EU Charter), and its' broader relevance, example in preventing behavioural discrimination/profiling and in preserving user autonomy and sovereignty. The next Section substantiates on this intersection of big data and antitrust, and puts forward the case for EU competition law intervention in such a privacy-centric context.

2. THE INTERSECTION OF BIG DATA AND COMPETITION LAW

As explored in the previous Section, extensive data gathering by dominant platforms creates multiple avenues for consumer exploitation, particularly by creating information asymmetries and degrading privacy. A key question here, which has recently attracted increasing attention, is – *is competition law the right tool to address such harmful implications, especially privacy, of data-related conducts*?

This Section explores this question as follows. Part 2.1 highlights key normative considerations; specifically those pertaining to the goals of EU competition law, and its' intersection with data and consumer protection. Part 2.2 explores how privacy and data collection have been historically assessed by antitrust authorities, and recent practical developments in this sphere. This discussion will highlight the significant intersection of big data and competition law, and how user privacy can (and in fact, should) be addressed using appropriate antitrust tools.

2.1. KEY NORMATIVE CONSIDERATIONS

There are two key considerations in the ongoing debate regarding the intersection of big data and antitrust. First, whether these issues fit within the remit of EU competition law goals; and second, if the applicability of consumer/data protection laws excludes antitrust intervention in any case.

EU competition law goals

It is often argued that antitrust has a price-centric objective, guided purely by economic principles and goals; which lacks the tools to account for non-price, data-related parameters and is also unsuitable for achieving non-economic goals like privacy.[61]

However, this purist approach reliant on a very narrow interpretation of the consumer welfare standard, is debatable. First, although 'price' has been a visible antitrust focus area, the consumer welfare standard is broader and also includes other parameters (like quality, consumer choice and innovation[62]), which need to be accounted for '*at least as much as narrow financial considerations'*.[63] Specifically, user privacy often constitutes an attribute of product quality in the zero-price data economy (further discussed in Section 6); and so, can directly be linked to consumer welfare. Therefore, ensuring platforms' privacy-quality in data markets arguably falls squarely within the goals of EU competition law.

Second, the goals of EU competition law are not restricted to just consumer welfare, but also include fairness, consumer decision-making sovereignty, democracy etc.; and therefore can include data-related issues like privacy (Ezrachi).[64] Additionally, as noted by Holmes, the starting point for any analysis of treaties should be their 'constitutional'

[61]Melamed and Petit, 'The Misguided Assault on the Consumer Welfare Standard in the Age of Platform Markets' (2019) 54 Review of Industrial Organisation 741.

[62]'Statement on Commission decision to fine Google euro 2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service' (*EC*, 27 June 2017) < http://europa.eu/rapid/press-release_STATEMENT-17-1806_en.htm>; Commission Guidance on its Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C/45/7, para 11.

[63]Holmes, 'Climate change, Sustainability, and Competition law' (2020) 8(2) Journal of Antitrust Enforcement 354, 362.

[64]Ezrachi, 'The Goals of EU Competition Law and the Digital Economy' (2018) BEUC Discussion Paper 14.

provisions or '*the bits at the beginning that explain what they are all about'*.[65] In this context it has been noted how data protection is recognized in Article 16 TFEU and also as a fundamental right under the EU Charter (Article 8). And, as the EU is under a duty to promote fundamental rights (Article 51, EU Charter), data protection falls within the realm of EU competition law.[66] Similarly, some commentators have also noted how as a fundamental right, data protection can also exercise an external constraint on EU competition law and shape its application accordingly.[67]

Therefore, when viewed from a broader-than-price lens - a view which is garnering increasing recognition - privacy-related issues fall within the remit of EU competition law (especially as a quality parameter).[68]

Notably, there are multiple ways in which data-related issues can manifest in antitrust assessments and necessitate the use of competition law tools.[69] For instance, ex-ante merger control can address issues pertaining to data amalgamation, enhanced abilities to acquire/use data anti-competitively, privacy degradation, reduced innovation in privacy etc.[70] Article 101

[65]Holmes (n 63) 359.

[66]Kuner et al, 'When two worlds collide: the interface between competition law and data protection' (2014) 4(4) International Data Privacy law 247, 248; Abstract in Irakiza, 'The Charter of Fundamental Rights, the Aims of EU Competition Law and Data Protection: Time to Level the Playing Field' (2021) Singapore Journal of Legal Studies 39 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3858349> accessed 25 June 2021.

[67]Costa-Cabral and Lynskey, 'Family ties: The intersection between data protection and competition in EU law' (2017) 54 CML Rev. 11, 23.

[68]Robertson, Antitrust Law and Digital Markets (n 3) 14.

[69]Vestager, 'Keynote Speech' (The Florence Competition Summer Conference, Hybrid, 24 June 2021) <https://www.youtube.com/watch?v=p0fjzCVK6Bg> accessed 2 July 2021.

[70]Pepper and Gilbert, 'Privacy Considerations in European Merger Control: A Square Peg for a Round Hole' (2015) 5 Antitrust Chronicle Competition Policy International.

TFEU can address anticompetitive licensing agreements for data, and agreements deciding the level of privacy offered or deciding to provide zero-price services to maximize data collection.[71] Article 102 TFEU, which sanctions a dominant firm's abuse of market power, can tackle exclusionary and exploitative data-related conducts. Exclusionary conducts in the data economy include behaviours like refusal to provide data, giving discriminatory access to data, exclusive contracts, tying of access to personal user data to other products and cross-usage of datasets.[72] Example, Facebook using its data advantage to create superior market intelligence and then copying or killing nascent competitive threats, would be an exclusionary data-related abuse.[73] Exploitative abuses under Article 102 TFEU include conducts like extensive data harvesting (the subject-matter here), behavioral discrimination, data-related manipulation, restriction of consumer choice etc.

The intersection of competition, data protection and consumer laws

The data economy comprises of several market failures like information asymmetries, users' behavioral biases, lack of transparency, unfulfilled consumer privacy preferences, the Privacy Paradox (discussed in Section 6), default opt-ins necessitated by the bundling of digital services with personal data etc.[74] These market failures are unlikely to be rectified by market incentives alone and warrant intervention, which can come from different spheres;

[71]Moorcroft and Le Strat, 'The rise of big data: The intersection between competition law and customer data' (2018) 38 Licensing Journal 8, 9.

[72]French-German Report (n 10) 17-30.

[73]US HJR (n 26) 160.

[74]Economides and Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective' (2021) Journal of Competition Law and Economics (forthcoming) 1.

particularly, with significant scope for antitrust, data protection and consumer law to play a complementary role. As observed by Andreas Mundt:

> *Data protection, consumer protection and the protection of competition interlink where data, as in Facebook's case, are a crucial factor for the economic dominance of a company.*[75]

Here, data protection legislation (ex., the GDPR /envisaged ePrivacy Regulation[76]) is essential to provide baseline privacy protection to individuals online; and similarly, consumer policy enforcement (ex., the Unfair Contractual Terms Directive (UCTD)[77] and Unfair Commercial Practices Directive (UCPD)[78]) is a pre-requisite for addressing asymmetric information. Simultaneously, competition law also has a complementary role in adding a significant layer of protection against exploitative data harvesting, example by ensuring a healthy market structure (through merger enforcement) and sanctioning abuses by dominant platforms (Article 102 TFEU). Therefore, all three regimes are significant, and in situations where the constituent legal requirements are fulfilled, a dominant firm might violate them all.[79] Additionally, far from the application of one regime precluding the use of another, these regulatory frameworks have closely aligned goals in the digital ecosystem, with several avenues for simultaneous application. For instance, in the German Facebook case in holding

[75]'Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive' (*Bundeskartellamt*, 19 December 2017) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html> accessed 27 May 2021.

[76]Commission Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications COM/2017/010 final - 2017/03 (COD) (ePrivacy Regulation).

[77]Council Directive (EEC) 93/13 on unfair terms in consumer contracts [1993] OJ L95/29.

[78]Council Directive (EC) 2005/29 concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149.

[79]Costa-Cabral and Lynskey (n 67) 14, 23.

that it '*has no serious doubts*' that Facebook's terms of use are abusive; the German Federal Court of Justice specifically observed that in addition to violating the GDPR, Facebook's terms also constitute anticompetitive exploitation in light of switching costs and lock-in effects.[80]

A clear illustration of how market power and privacy interact and warrant antitrust intervention despite the existence of data protection legislations, is demonstrated by the GDPR's somewhat lopsided impact and the potential role to be played by competition law in this context. Specifically, although the GDPR has provisions for limiting third-party tracking, these are unduly onerous on smaller platforms whilst large platforms have used the framework to reinforce their own dominance; for instance, Google can now collect more data than the pre-GDPR era.[81] This can be attributed to a few key reasons:

The GDPR primarily emphasizes on individual rights without placing these rights in the broader context. And although such user empowerment and strengthened consent requirements are important; in the data economy, which is highly concentrated and where information asymmetries are significant, such empowerment and '*sole focus on micro-level harms'* is insufficient.[82] Notably, when users are dealing with monopolies, individual control over personal data and data protection concepts like consent become '*more and more illusory'*.[83] Further, consent-based data collection under the GDPR creates comparative

[80]Lomas (n 1).

[81]Greif, 'Study: Google Is the Biggest Beneficiary of the GDPR' (*Cliqz*, 10 October 2018) <https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr> accessed 27 May 2021.

[82]Graef, 'Speech on Data Silos' (The Florence Competition Summer Conference, Hybrid, 25 June 2021).

[83]EDPS Preliminary Opinion, *Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy* (2014) 35 (2014 EDPS Opinion); Kuner et al (n 66) 247.

advantages to diversified/large firms which collect their own data, whilst creating disproportionate transaction costs for less diversified or new firms, thereby strengthening large data controllers.[84] Studies have also found that '*market share is strongly correlated with using intrusive permissions... [and] ... acquiring more data*'.[85] Additionally as also noted by the CMA, big platforms could also be interpreting the GDPR in a way which favours their business models, instead of in a way which gives users control of their data.[86]

As such, the GDPR's effectiveness is clearly influenced by market power and ignoring this aspect further individualizes users' responsibility for their privacy protection, without addressing the more systemic imbalances prevalent in the online economy. Additionally, in an era of big data, where everyone and everything is connected, dominant platforms' data collection creates externalities and macro-level harms which the GDPR is ill-equipped to address; but, can be targeted by antitrust.[87] This is particularly the case given how competition law is *meant* to constrain the unbridled power of large companies – both in price and non-price contexts, and is one of the sharpest tools available for this purpose. Therefore, antitrust is often perceived as the '*silver bullet*' in complementing data protection rules and addressing privacy problems in the platform economy; example, by injecting competition, curtailing abuse and facilitating individual choice.[88]

[84]Gal and Aviv, 'The Competitive effects of the GDPR' (2020) 16(3) Journal of Competition Law & Economics 349, 350.

[85]Esayas, 'Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law' (2018) 8(3) International Data Privacy Law 181, 184.

[86]CMA Digital Advertising Report (n 50) para 5.316.

[87]Graef speech (n 82).

[88]Kuner et al (n 66) 247.

However, there are two important caveats here. First, a breach of data protection/consumer law is neither directly sanctionable nor a necessary requirement for an antitrust infringement, and all other conditions relevant from a competition law perspective would also need to be satisfied.[89] Second, such complementarity isn't free from challenges. For instance, although Google's recent plan to remove third-party cookies from Chrome is welcome from a privacy perspective, it has attracted significant antitrust scrutiny as an exclusionary abuse.[90] There has also been come controversy regarding Apple's privacy-protecting App Tracking Transparency feature in the new iOS 14 software, which requires specific user opt-in for data collection and tracking. Specifically, antitrust complaints have been filed in France (where the complaint was rejected) and Germany, on the grounds that it constitutes an exclusionary abuse of dominance.[91] Similarly, there could also be a conflict between the data-sharing obligations under Article 102 TFEU and the GDPR, tensions caused by data-driven efficiencies, positive privacy implications of consolidation etc.

[89]Robertson (n 34) 167.

[90]'UK Watchdog To Probe Google Chrome Changes Over Antitrust Concerns' (*CPI*, 10 January 2021) <https://www.competitionpolicyinternational.com/uk-watchdog-to-probe-google-chrome-changes-over-antitrust-concerns/ > accessed 27 May 2021; 'Google's New Privacy Moves Causes US Antitrust Concerns' (*CPI*, 18 March 2021) <https://www.competitionpolicyinternational.com/googles-new-privacy-moves-causes-us-antitrust-concerns/> accessed 27 May 2021; 'EU's Vestager Says Google's Planned Removal Of Third-Party Cookies Is An Antitrust Concern' (CPI, 25 April 2021) <https://www.competitionpolicyinternational.com/eus-vestager-says-googles-planned-removal-of-third-party-cookies-is-an-antitrust-concern/> accessed 27 May 2021.

[91]Espinoza, 'German groups file Apple antitrust complaint as it makes privacy changes' (*Financial Times,* 26 April 2021) <https://www.ft.com/content/0a48d9aa-244b-4945-b2a0-01c68683544a> accessed 27 May 2021; Lomas, 'France's competition authority declines to block Apple's opt-in consent for iOS app tracking' (*TechCrunch*, 17 March 2021)<https://techcrunch.com/2021/03/17/frances-competition-authority-declines-to-block-apples-opt-in-consent-for-ios-app-tracking/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAItEzT9YjqLzez6Efli-Urw8prP-Lwp0TTKpHkyE2uHzUL7EdvtnnDEwyXqPa_fShYFRaaart3jMnd8HHyCsp5K7bXUSkH2CNFdSWFeOwp5ATlTT1jFMqb_PaoZLWTbZbv9JQfsVbWnoqEn7ndPdbSoDRzzTcNa_CqrqqEh2fY5> accessed 27 May 2021.

These challenges, however, don't preclude the three areas from playing a complementary role. Instead, what is required is a '*more holistic approach to enforcement*' and systematic dialogue among competition, consumer and data protection authorities[92] (discussed in Section 7).

Having established the normative justification for this antitrust-privacy intersection, the following Part explores practical enforcement in this area.

2.2. ENFORCERS' PRACTICAL APPROACH

As discussed above, there are strong normative justifications for antitrust intervention in the data economy, which can be in various capacities - data as a source of market power, privacy concerns, ensuring access to data for smaller competitors etc. This thesis focuses specifically on the privacy and data collection aspects of such issues, and this Part explores competition enforcers' practical approach towards the same.

Historically, antitrust authorities have had a tendency to keep competition law separate from issues like privacy and data collection. In *Asnef-Equifax*[93], which pertained to a data sharing agreement, the ECJ observed that privacy concerns as such are not within the scope of antitrust intervention and could be resolved under data protection laws instead. Similarly, in *Facebook/Whatsapp*[94] the EC primarily focused on possible foreclosure, whilst relegating all privacy-related concerns to the data protection sphere. The same approach was adopted by

[92]2014 EDPS Opinion (n 83) 37.

[93]Case C-238/05, *Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios* [2006] ECR I – 11145.

[94]*Facebook/WhatsApp* (Case M.7217) Commission Decision C(2014)7239 [2014] OJ C417/4, para 164.

the Commission in *Google/DoubleClick*[95]; and despite a powerful dissenting judgment[96], the FTC also concluded that the merger had no adverse impact on privacy.[97] Similarly, in *Google/Fitbit* the Commission held that privacy concerns are better addressed by other regulatory tools like the GDPR's consent requirements.[98] Such reliance on data protection laws was also made in cases involving increased potential for data combination by the merged entity (*Microsoft/LinkedIn*[99], *Verizon/Yahoo*[100] etc.). Importantly, the EC appears to have completely ignored the implications of third-party tracking in merger assessments[101]; a key example being *Microsoft/LinkedIn*, which resulted in a combined third-party tracking presence of 42.81%.[102] Additionally, in some cases competition authorities have not addressed data combination and privacy related issues at all, despite their considerable significance.[103]

However, such sole reliance on data protection laws, whilst ignoring the combined entities' market power and its long-term implications on data collection and privacy has

[95]*Google/DoubleClick* (Case M.473) Commission decision C(2008) 927 [2008] OJ C184/10, para 368.

[96]Pamela Jones Harbour, *Dissenting Statement – In the Matter of Google/DoubleClick* (File No 071-0170, 20 December 2007) <https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf> accessed 27 May 2021.

[97]FTC, *Statement Concerning Google/DoubleClick* (File No 071-0170, 20 December 2007) 2-3 < https://www.ftc.gov/public-statements/2007/12/statement-federal-trade-commission-concerning-googledoubleclick > accessed 27 May 2021.

[98]'Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions' (*Commission*, 17 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484> accessed 27 May 2021.

[99]*Microsoft/LinkedIn* (Case M.8124) Commission Decision C(2016) 8404 [2016] OJ C388/4, para 255.

[100]*Verizon/Yahoo* (Case M.8180) Commission Decision C(2016) 8978 [2016], para 90.

[101]Economides and Lianos (n 74) 3 (examples include Adobe/Lyvefire (2016), Facebook/Liverail (2014), Alibaba/Umeng (2013) etc.).

[102]Ezrachi and Robertson (n 2) 3.

[103]Binns and Bietti (n 38) 32 (discussing *Microsoft/Yahoo*); OECD Data-Rights Report (n 31) 27, 28 (discussing *Facebook/Instagram* and *Google/Nest Lab*).

proven to be somewhat short-sighted, with various platforms engaging in recidivism. For instance, once Google and Facebook acquired substantial market power and no longer feared consumer backlash, they infringed commitments made to competition authorities during their respective mergers and significantly degraded consumer privacy by combining data across services.[104] The companies have also otherwise repeatedly infringed their privacy commitments; for instance in respect of Facebook's violations, District Court Judge Timothy Kelley observed that '*the unscrupulous way in which….Facebook violated both the law and the administrative order is stunning*.'[105] The EC's recent approval in *Google/Fitbit* has also attracted much criticism - Tommaso Valletti (the Commission's former chief competition economist) noted how '*we don't understand the consequences of data*' and in approving such transactions and given the GDPR's lack of implementation '*we are creating a system that is out of control*'.[106] Similarly, Shoshana Zuboff also noted how *Google/Fitbit* '*should be reconsidered immediately and never repeated'*.[107]

Therefore, there is a strong case to alter the traditional approach of keeping competition law and privacy/data collection issues separate; a notion gaining increasing acknowledgement among antitrust enforcers. Examples include Germany's Facebook decision and the BkM's recent antitrust investigation into Google's data processing terms[108];

[104]US HJR (n 26) 158, 210.

[105]*United States v Facebook Inc*., No. CV 19-2184 (TJK), 4 (D.D.C. 2020), 1 <https://www.courtlistener.com/opinion/4748088/united-states-v-facebook-inc/> accessed 27 May 2021.

[106]Scott (n 8).

[107]Stolton, 'Don't ignore platforms 'combining services' in Digital Markets Act, Netherlands says' (*Euractiv,* 17 February 2021) <https://www.euractiv.com/section/digital/news/dont-ignore-platforms-combining-services-in-digital-markets-act-netherlands-says/> accessed 31 May 2021.

[108]Bundeskartellamt (n 7).

legislative changes in Germany and renewed merger notification thresholds (to value-based from just turnover-based) in Austria and Germany[109]; global reports on data and antitrust[110]; FTC's Hearings on Competition and Consumer Protection[111]; the JFTC's focus on scrutinizing digital platforms' handling of consumer data[112]; the Indian and Turkish NCAs actions against Whatsapp's use being made conditional on user data-sharing with Facebook for being potentially exploitative[113] etc. At the EU level, the Commission observed in *Microsoft/LinkedIn*, that privacy-related questions *can* be taken into account in competition assessments to the extent they are perceived as a significant factor of quality.[114] This is a notable departure from earlier decisions like *Facebook/Whatsapp*, where the Commission noted that '*[a]ny privacy-related concerns flowing from the increased concentration of data….do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules*'.[115] Notably in a recent Executive Order, US President Biden also

[109]Ezrachi and Robertson (n 2) 7.

[110]French-German Report, Cremer Report, Furman Report, Stigler Report, 2014 EDPS Opinion, OECD Data-Rights Report etc.

[111]FTC, *Hearings on Competition and Consumer Protection in the 21st Century* (October 2020) < https://www.ftc.gov/system/files/documents/reports/commission-report-hearings-competition-consumer-protection-21st-century/p181201internationalhearingreport.pdf> accessed 27 May 2021.

[112]Sakamaki, 'Digital platforms' handling of consumer data to be scrutinized under antitrust law in Japan' (*Mlex,* 29 August 2019) <https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/antitrust/digital-platforms-handling-of-consumer-data-to-be-scrutinized-under-antitrust-law-in-japan> accessed 27 May 2021.

[113]Singh and Mishra, 'CCI's Investigation into WhatsApp Service Policy Update: Mapping the Scope of Regulation of Privacy Policy vis-à-vis Competition Act, 2002' (*Kluwer Competition Law Blog,*19 April 2021) < http://competitionlawblog.kluwercompetitionlaw.com/2021/04/19/ccis-investigation-into-whatsapp-service-policy-update-mapping-the-scope-of-regulation-of-privacy-policy-vis-a-vis-competition-act-2002/> accessed 27 May 2021; Ozer, 'The WhatsAppocalypse: Turkish Competition Board Launches In-depth Investigation Against Facebook And WhatsApp' (*Mondaq* 12 January 2021) < https://www.mondaq.com/turkey/antitrust-eu-competition-/1024634/the-whatsappocalypse-turkish-competition-board-launches-in-depth-investigation-against-facebook-and-whatsapp> accessed 27 May 2021.

[114]'Commission approves acquisition of LinkedIn by Microsoft, subject to conditions' (*Commission*, 6 December 2016) <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284> accessed 27 May 2021.

[115] Facebook/Whatsapp (n 94) para 164.

stressed on the greater scrutiny of mergers '*with particular attention to the….accumulation of data…and the effect on user privacy';* and recognizing that big tech were '*gathering too much personal information*', the Order also encouraged the FTC '*to establish rules on…the accumulation of data*'.[116]

Accordingly, we witness a steadily growing acknowledgment of the privacy-competition intersection, and strong support for effective Article 102 TFEU enforcement in curbing exploitative data collection and privacy degradation. Before exploring suitable ToH for such intervention and diving into the particulars of the data economy, it is crucial to understand the context behind exploitative abuses (a controversial area of antitrust) and how it has evolved over the years. This is discussed in the next Section.

[116]'Fact sheet: Executive Order on Promoting Competition in the American Economy' (*The White House*, 9 July 2021)< https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/ > accessed 15 July 2021.

3. EXPLOITATIVE ABUSES UNDER ARTICLE 102 TFEU

Having discussed dominant firms' data collection practices and the intersection thereof with competition law, we now move on to explore exploitative abuses under Article 102 TFEU – the antitrust tool being focused on in this thesis.

At the outset it must be noted that there are various steps involved in establishing an infringement of Article 102 TFEU like defining the relevant market, establishing market power and dominance etc. This thesis doesn't discuss such issues and assumes that all necessary conditions to establish dominance have been fulfilled, and also doesn't discuss the notion of exclusionary abuses. The main focus here is exploitative abuses, in light of dominant firms' data harvesting practices.

This Section provides some essential context to this traditionally controversial area of antitrust. Part 3.1 provides a general background to exploitative abuses. Part 3.2 discusses policy reasons for enforcers' traditionally low intervention appetite in this area. Part 3.3 highlights the evolution of exploitative abuses (i.e., around excessive pricing) and practical enforcement challenges; and Part 3.4 discusses renewed attention in this area in digital markets. The application of exploitative abuses specifically in the data economy is discussed in the next Section.

3.1. BACKGROUND

Exploitative abuses are unilateral behaviors by dominant firms which distort competition by directly harming final consumers rather than excluding competitors, example by imposing excessive prices or other unfair terms on consumers. It is a controversial area of competition law enforcement, with different jurisdictions adopting significantly varied approaches depending on how their respective antitrust philosophies and policy goals have evolved.[117]

A key difference, for instance, is between the US and EU approaches. The US doesn't sanction exploitative conducts under its antitrust provisions; and as clarified by the US Supreme Court in *Trinko*[118], companies with market power may not only charge excessive prices, but in fact '*the opportunity to charge monopoly prices – at least for a short period – is what attracts "business acumen" in the first place'* and is an '*important element of the free-market system*'.[119] This rationale applies to excessive pricing and other forms of consumer exploitation.[120]

In contrast, EU competition law sanctions exploitative abuses of dominance through the Article 102 TFEU framework. Specifically, Article 102(a) prohibits dominant undertakings from '*directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions*'; thereby, ensuring that they don't directly harm consumers.[121] The

[117]Gal, 'Monopoly Pricing as an Antitrust Offense in the US and the EC: Two Systems of Belief About Monopoly?' (2004) 49 Antitrust Bulletin 343-384.

[118]*Verizon Communications Inc v Law Offices of Curtis v Trinko LLP*, 540 U.S. 398 (2004) (*Trinko*).

[119]ibid 7.

[120]Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct – The German Facebook Case*'* (2021) 66(2) The Antitrust Bulletin 276,280.

[121]OECD, *Abuse of dominance in digital market*s (2020) 49 (OECD AoD).

key rationale for sanctioning such exploitative conduct is to ensure that the monopolist doesn't use its position to '*reap trading benefits which it would not have reaped if there had been normal and sufficiently effective competition'*.[122] Interestingly, the *travaux préparatoires* of the Rome Treaty indicates that the initial intention behind Article 102 TFEU was primarily to sanction exploitative abuses.[123]

A recent example of such enforcement by the EC is its excessive pricing case against Aspen.[124] Additionally, NCAs in Europe have also been particularly active in pursuing excessive pricing cases in the energy and pharmaceuticals sector. For instance, the Dutch NCA is currently investigating Leadiant's price rises for CDCA[125], the Danish NCA found CD Pharma guilty of excessively pricing Syntocinon (decision upheld on appeal)[126], the Italian NCA's case against Aspen[127] etc. The UK has also pursued similar cases. Example, in 2016 the CMA fined Pfizer and Flynn £90 million for excessive pricing, and following a few

[122]Case C-27/76 *United Brands Company and United Brands Continentaal v Commission* [1978] ECR 1978-00207, para 249.

[123]Akman, 'Searching for the Long-Lost Soul of Article 82 EC' (2009) 29(2) Oxford Journal of Legal Studies 267,271.

[124]'Antitrust: Commission opens formal investigation into Aspen Pharma's pricing practices for cancer medicines' (*Commission,* 14 May 2017) < https://ec.europa.eu/commission/presscorner/detail/es/IP_17_1323> accessed 27 May 2021.

[125]'ACM extends its investigation into orphan drug CDCA-Leadiant' (*ACM,* 29 June 2020) <https://www.acm.nl/en/publications/acm-extends-its-investigation-orphan-drug-cdca-leadiant> accessed 27 May 2021.

[126] 'The Maritime and Commercial Court: CD Pharma has abused its dominant position by charging an excessive and unfair price for the drug Syntocinon' (*Danish Competition and Consumer Authority*, 3 March 2020) < https://www.en.kfst.dk/nyheder/kfst/english/judgements/20200302-the-maritime-and-commercial-court-cd-pharma-has-abused-its-dominant-position-by-charging-an-excessive-and-unfair-price-for-the-drug-syntocinon/> accessed 27 May 2021.

[127]'Italian Competition Authority fines Aspen for excessive anticancer drug price increase' (*Ashurst*, 11 November 2016) <https://www.ashurst.com/en/news-and-insights/legal-updates/italian-competition-authority-fines-aspen-for-excessive-anticancer-drug-price-increase/ > accessed 5 June 2021.

appeals the case has now been remitted to the enforcer.[128] It also recently fined firms £260 million for excessively pricing hydrocortisone tablets (which witnessed a price increase of over 10,000%), and is investigating the pricing of liothyronine by Concordia.[129]

Importantly however, this recent spike in exploitative abuse cases - particularly at the EU level - is more exception than norm. Generally speaking, such cases have rarely been pursued and instead, majority of the Commission's enforcement under Article 102 TFEU so far has been in context of exclusionary conducts. The EC's enforcement priorities in this regard are also evident from the Commission's Guidance on Article 102 TFEU which only covers exclusionary conduct, while explicitly leaving out exploitative abuses.[130]

3.2. LIMITED INTERVENTION APPETITE - POLICY REASONS

There are various policy reasons for the EC's limited intervention when it comes to exploitative abuse cases.[131]

A key consideration is *the belief that markets are self-correcting.* It is argued that even if firms can charge excessive prices now, it will either incentivize new entry or the fear of new entrants would constrain the monopolist's power to raise prices and the market will correct

[128]'Phenytoin sodium capsules: suspected unfair pricing' (*CMA*, 18 December 2015) < https://www.gov.uk/cma-cases/investigation-into-the-supply-of-pharmaceutical-products> accessed 27 May 2021.

[129]'CMA finds drug companies overcharged NHS' (*CMA*, 15 July 2021) <https://www.gov.uk/government/news/cma-finds-drug-companies-overcharged-nhs > accessed 16 July 2021; 'Liothyronine tablets: suspected excessive and unfair pricing' (*CMA*, 25 October 2016) < https://www.gov.uk/cma-cases/pharmaceutical-sector-anti-competitive-conduct> accessed 27 May 2021.

[130]Commission Guidance (n 62) para 7.

[131]Donoghue and Padilla, *The Law and Economics of Article 102 TFEU* (2nd edn, Hart Publishing 2013) 735, 762.

itself. This self-correcting nature of excessive pricing conducts was also stressed upon in the UK OFT Guidelines on Assessment of Individual Agreements and Conduct, as per which:

> *Excessive prices may be considered to be an abuse only if they have persisted in the absence of continuing successful innovation and/or without stimulating successful new entry or a significant loss of market share.*[132]

This has historically been the popular position within the antitrust community, and a key argument against sanctioning excessive prices. Additionally, in the rare cases where the market would not eventually self-correct, it has been noted that ex-ante price regulation is better suited than ex-post antitrust enforcement.[133] However importantly, this position isn't entirely uncontested; for instance, it has been argued that high prices will not attract new entrants because they will consider expected post-entry prices rather than the high pre-entry ones when deciding whether to enter.[134]

Related to the market self-correction argument is the perception of *error-cost frameworks* in competition law. By way of background, the finding of harm to competition when there is none, are 'false positives', and findings that no harm to competition occurred when they have in fact occurred are categorized as 'false negatives'. Traditionally, false negatives have been viewed as preferable compared to false positives.[135] The key rationale here is that over-enforcement of competition law can be very costly and is capable of inflicting irreversible consumer and broader economic harm; whereas, under-enforcement is less costly

[132]Ezrachi and Gilo 'Are Excessive Prices Really Self-Correcting?' (2008) 5(2) Journal of Competition Law and Economics 249, 254.

[133]Donoghue and Padilla (n 131) 763.

[134]Ezrachi and Gilo (n 132) 255.

[135]Manne and Wright, 'Google and the Limits of Antitrust: The Antitrust Case Against Google' (2011) 34(1) Harvard Journal of Law and Public Policy 171, 176.

and will be corrected by the market itself, example through innovation or other market developments.[136] This assumption permeates all areas of competition law, but is particularly powerful in cases concerning exploitative abuses. This can be attributed to the strength of the market self-correction argument in such cases, the uncertainties regarding competition harms caused by exploitative behavior and the ambiguous implications of related intervention on long-term welfare effects.[137]

Another key argument is that such intervention would *discourage innovation*. It is contested that if firms are sanctioned for raising prices and reaping the rewards of their dominant position, they will be dissuaded from striving to develop superior products or cost savings in the first place and their incentive to innovate would be hampered; thereby, resulting in a detrimental impact on competition and consumers.[138]

Underenforcement can also be attributed to the *risk of price/market regulation.* It is argued that in deciding an appropriate benchmark for excessiveness, courts will necessarily have to determine what the 'fair' or correct level of pricing should be, which goes against the basic premise of a market economy. As observed by the US Supreme Court in *Pacific Bell v Linkline*[139], in identifying proper price and other contractual conditions like quantity, courts will effectively be assuming the day-to-day control characteristic of a regulatory agency; a

[136]ibid.

[137]Evans and Padilla, 'Excessive Prices: Using Economics to Define Administrable Legal Rules' (2005) 1(1) Journal of Competition Law & Economics 97, 120.

[138]*Trinko* (n 118).

[139]*Pacific Bell Telephone v Linkline Communications*, 129 S.Ct. 1109, 1122 (2009).

role for which they are ill-suited. Such market regulation is considered highly undesirable, and constitutes a key policy objection to sanctioning exploitative conducts.[140]

In light of these policy reasons, many authors have argued that the prohibition of exploitative abuses should not be applied at all; and, in any case, such concerns have severely restricted enforcement action in this area in Europe. Additionally, as discussed below, the few exploitative abuse cases which have been pursued so far have raised practical concerns and further deterred the Commission from sanctioning such behaviour.

3.3. THE EVOLUTION OF EXPLOITATIVE ABUSES AND PRACTICAL CHALLENGES

This Part explores the evolution of exploitative abuses in Europe, and also highlights the key enforcement challenges underlying such cases.

In this context, there are two important points. First, enforcement under Article 102(a) TFEU has primarily been in relation to excessive pricing. However, these cases have such a complicated and high burden of proof that the EC has seldom been able to satisfy the same, thereby deterring Commission activity in this sphere. Second, although Article 102(a) TFEU also prohibits the imposition of unfair trading conditions, such conducts are pursued even less frequently than excessive pricing. Additionally, there is also a paucity of cases (and much uncertainty) regarding other non-pricing exploitative conducts like the deterioration of quality, consumer choice and innovation. These points are further detailed below. Please note, what follows is not a comprehensive discussion of case law, but the leading decisions in this

[140] *At the Races Limited v The British Horse Racing Limits and others* [2007] EWCA Civ 38, para 217.

sphere to highlight defining principles and practical challenges underlying exploitative abuses; which are then referenced in subsequent Sections.

Evolution of exploitative abuses: focus on excessive pricing

Excessive pricing is often referred to as the 'classic' exploitative abuse case. This focus on pricing can be attributed to competitions law's traditionally price-centric approach and the belief that antitrust tools are best applied within a quantifiable, price-based framework (the so-called 'mathematization' of competition law).[141] Although non-price factors like quality and consumer choice are widely recognized as important elements of competition, it is argued that they can cause significant uncertainty and ambiguity; and therefore, have traditionally always been avoided.[142] Consequently, most exploitative abuse cases have evolved around excessive pricing.

The CJEU first observed the EC's power to sanction excessive pricing in *General Motors,* where it regarded the price to be abusive as it was '*excessive in relation to the economic value of the service provided'.*[143] Thereafter, the CJEU established key principles on excessive pricing in *United Brands*[144] (UB), which is still the leading case in Europe on this subject. Here, the Court confirmed that prices are excessive when they have '…*no reasonable relation to the economic value of the product*….'; and, set out the following two-

[141]Kokkori and Lianos, *The reform of EC Competition law: New Challenges* (Kluwer Law International 2009) 57.

[142]OECD AoD (n 121) 50.

[143]Case C-26/75 *General Motors Continental NV v Commission of the European Communities* [1975] ECR 1975-01367, para 12.

[144]*United Brands* (n 122).

step assessment to determine the excessiveness of price: (i) the difference between the costs incurred and the price charged had to be excessive, and (ii) the price had to be either unfair in itself or when compared to that of competing products.[145] Therefore, both excessiveness and unfairness need to be established in an excessive pricing case. This UB framework is the seminal test in this context.

In practice however, the UB test is very complicated to implement and sets out a very high and convoluted standard of proof. It is also riddled with practical difficulties like assessing the cost structure/degree of profitability, identifying competitive prices etc. Importantly, and as noted in UB itself, this test is not the only approach and '*other ways'* can also be used to establish the abuse of excessive pricing.[146] This includes using comparative benchmarks like prices charged in other product/geographic markets by the dominant undertaking, pricing by other undertakings in the same or related markets, the evolution of pricing over time etc.[147]; an approach which has been used in various cases like *AKKA/LAA*[148], *Napp*[149] and *Pfizer/Flynn*[150]. However, this comparative approach also faces its own

[145]ibid paras 249-252.

[146]ibid para 253.

[147]Case C-177/16 *Autortiesību un komunicēšanās konsultāciju aģentūra v. Latvijas Autoru apvienība v Konkurences padome* [2017] ECLI:EU:C:2017:689 (AKKA/LAA), Opinion of AG Wahl, para 19.

[148]Paras 37, 38, 46, 50 and 51.

[149]1001/1/1/01 *Napp Pharmaceutical Holdings Limited and Subsidiaries v Director General of Fair Trading* [2002] CAT 1, paras 388, 392.

[150]*The CMA v Flynn Pharma Limited and Pfizer Inc* [2020] EWCA Civ 339 (Pfizer/Flynn), para 251.

enforcement challenges, like the difficulties in adjusting pricing across markets and making temporal comparisons in light of increased efficiencies and improvements in technology.[151]

Notably in its most recent Aspen case, despite strong findings of excessive pricing, the Commission didn't continue proceedings to reach an infringement decision, but accepted commitments under Article 9(1) of Regulation 1/2003 instead.[152] Such an approach reaffirms the EC's hesitance towards fully investigating complex excessive pricing conducts, and is in line with previous cases where the Commission has preferred commitments over an appealable infringement decision.[153]

Therefore, although exploitative abuses in the EU have primarily evolved around excessive pricing, the difficult standard of proof and practical challenges underlying the same have resulted in the Commission rarely sanctioning such conduct.[154]

[151]Botta and Wiedemann, 'EU Competition Law Enforcement Vis-À-Vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita' (2018) Max Planck Institute for Innovation & Competition Research Paper No. 18-08 < https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3184119> accessed 28 May 2021 (Terra Incognita).

[152]'Antitrust: Commission accepts commitments by Aspen to reduce prices for six off-patent cancer medicines by 73% addressing excessive pricing concerns' (*Commission,* 10 February 2021) < https://ec.europa.eu/commission/presscorner/detail/en/IP_21_524> accessed 28 May 2021.

[153]DLA Piper, 'Aspen: Quick Fix But Missed Opportunity' (*Kluwer Competition Law Blog*, 23 October 2020) <http://competitionlawblog.kluwercompetitionlaw.com/2020/10/23/aspen-quick-fix-but-missed-opportunity/ > accessed 28 May 2021. Cases mentioned include *Standard & Poor's* (Case COMP/39.592 dated 2011), Gazprom (AT.39816 dated 2018) etc.

[154]Terra Incognita (n 151) 6.

Unfair trading conditions and non-pricing exploitative abuses

Article 102(a) TFEU applies not just to excessive pricing, but also to other '*other unfair trading conditions*'. However, enforcement action pertaining to this category of abuse is even rarer than excessive pricing.

Some notable examples of such cases include unfair terms of sales for tickets to the 1998 Football World Cup in France that imposed higher burdens on non-French citizens than on French nationals[155], limiting the provision of a service for which there was consumer demand in *Deutsche Post*[156], take-it-or-leave-it clauses in *Duales Systems Deutschland (DSD)*[157], unfair terms against certain members of an association in *BRT/SABAM*[158] etc.

From these cases (also discussed in Section 5), certain general criteria in assessing the 'unfairness' of trading conditions (like unnecessary, disproportionate, unilaterally imposed etc.) can be deducted; however, these still fall short of a clear legal test or distinct threshold. Presumably given the underlying ambiguities and non-price elements of such cases, they are not an enforcement priority for the Commission. Similarly, other non-price parameters of competition like quality, consumer choice and innovation have also not seen any Article 102 TFEU enforcement so far.

[155]Case IV/36.888 *1998 Football World Cup Commission Decision* [2000] OJ L5/55.

[156]*Deutsche Post AG — Interception of cross-border mail* (Case COMP/C-1/36.915) Commission Decision 2001/892/EC [2001] OJ L331/40.

[157]*Duales System Deutschland (DSD)* (Case COMP/34.493) Commission Decision 2001/463/EC [2001] OJ L166/1.

[158]Case 127/73 *BRT v. SABAM* [1974] ECR 1974-00051 314.

Overall, the manner in which exploitative abuse cases - both pricing and non-pricing - have been decided over the years has created substantial enforcement challenges; and, has added to the Commission's reluctance in pursuing such conducts. However notably, there has been some renewed interest in this area in the digital sphere.

3.4. RENEWED ATTENTION IN THE DIGITAL SPHERE

Despite the general controversies associated with exploitative abuses in traditional markets, there has been some renewed interest in this sphere in the data economy.

Numerous reports and academic articles have acknowledged the exploitative nature of dominant platforms' anti-competitive conducts; and, how these practices (like data exploitation, abrupt changes to a platform's policies etc.) are becoming increasingly systemic.[159] Additionally, with the German Facebook case and the current BkM proceedings against Google, there has now also been enforcement action in this sphere. And although it is under German law, such enforcement is a striking development in the field of both exploitative abuses and the data economy; and has raised several interesting and debatable questions for competition law in general, and Article 102 TFEU in particular.

The rest of this thesis explores this realm of exploitative abuses as applied to dominant firms' data collection practices. Specifically, the next Section establishes the rationale for Article 102 TFEU enforcement in the data economy, and explores why traditional arguments against intervention in exploitative abuses (as discussed in this Section) don't apply in that

[159]OECD, *Big data: Bringing competition policy to the digital era* (Background Note DAF/ COMP, 2016) para 48; French-German report (n 10) 22-25; OECD Data-Rights Report (n 31) 29; US HJR (n 26) 51-57, 390; Stigler Report (n 25) 119; Ezrachi and Robertson (n 2); Terra Incognita (n 151).

context. It also introduces relevant ToH for such intervention, which are then detailed in Sections 5 and 6.

4. ARTICLE 102 TFEU AND EXPLOITATIVE DATA HARVESTING – THE RATIONALE FOR INTERVENTION

Having discussed exploitative abuses and associated controversies in traditional markets, this Section now focuses on the specifics of the digital economy and explores the rationale for Article 102 TFEU intervention in exploitative data collection practices.

Part 4.1 introduces potential ToH and highlights the importance of non-price factors as key elements of competition. Part 4.2 explores how challenges associated with exploitative abuses in traditional markets are less relevant in the data economy; and also highlights key filters used in traditional exploitative abuse cases and their applicability in digital markets.

4.1. POTENTIAL THEORIES OF HARM

At the outset, it is useful to note that Article 102 TFEU intervention against exploitative data harvesting can be justified using two potential ToH; specifically, (i) excessive data harvesting as an Article 102 TFEU violation, and (ii) privacy-quality degradation as an exploitative abuse of dominance. The specifics of each of these, including their feasibility and associated challenges are detailed in Sections 5 and 6 respectively.

Importantly however, these theories go beyond 'prices' to include non-price elements of competition, especially product/service quality. Although traditionally the notion of exploitative abuses has evolved around pricing, there is no reason to restrict its enforcement

to price-centric contexts. This is particularly the case in digital markets where many services are provided for free and so, there is no price-related benchmark to measure consumer harm against. In such cases it is imperative to assess consumer harms using other benchmarks like quality, consumer choice and innovation.[160] These non-price elements (especially quality), ways in which they can be incorporated in competition assessments and associated challenges are further detailed in the following Sections.

Having introduced relevant ToH, let us now consider the rationale for Article 102 TFEU intervention against exploitative data harvesting in the platform economy.

4.2. TRADITIONAL ARGUMENTS AGAINST INTERVENTION IN EXPLOITATIVE ABUSES DON'T APPLY TO THE DATA ECONOMY

The previous Section explored various reasons for the Commission's low intervention appetite in exploitative abuse cases in traditional markets. However as discussed below, these arguments don't hold the same weight when viewed in context of the digital economy, particularly in context of data harvesting conducts.

Will markets self-correct?

In context of the digital economy, proponents of the market self-correcting point to the dynamic nature of technology, the role of disruptive innovation, and firms' strong investments in research and development. In practice however, rapid self-correction in markets dominated

[160]OECD, *The Role and Measurement of Quality in Competition Analysis* (Policy Roundtables, 2013) (OECD Quality Report); Ezrachi and Stucke, 'The Curious Case of Competition and Quality' (2015) 3(2) Journal of Antitrust Enforcement 227, 228. *See also* n 62.

by large digital platforms, and especially in respect of firms' exploitative data collection practices, is unlikely.

At a broader level, the inherent features of digital markets like economies of scale and scope, network effects, negligible marginal costs, the self-reinforcing data advantage; all, result in a winner-takes-all (or most) dynamic and comprise high entry barriers, thereby protecting incumbents. Additionally, innovations in technology will also not support new dynamic entrants given that they can just easily be taken over by dominant platforms.[161]

Specifically in respect of firms' extensive data collection practices, it is also unlikely that the market will self-correct.[162] Given their advertising revenue-based business models, online platforms are motivated to collect and monetize as much user data as possible. As such, the market essentially incentivizes platforms to further deepen information asymmetries between themselves and the user, and use these asymmetries to their economic advantage. This is evident in how firms are increasingly developing manipulative interfaces or dark patterns, and blatantly disregarding user privacy. As noted by Stucke and Grunes: '*We are witnessing a competitive arms race for data (as opposed to more privacy)— the race to connect the 'data' bucket with the 'money' bucket… '*.[163]Additionally, online platforms rarely internalize the harms associated with consumer privacy and security breaches, negative externalities or potential misuses of data.[164] As such it is unlikely that privacy and data security

[161]Stigler Report (n 25), 81.

[162]Economides and Lioanis (n 74) 42.

[163]Stucke and Grunes (n 11) 1.

[164]Acquisti, Taylor and Wagman, 'The Economics of Privacy' (2016) 54(2) Journal of Economic Literature 442, 452.

problems will be solved by market incentives alone.[165] This is evidenced by how some key sophisticated platforms lack basic data protection features. For instance, Facebook stored millions of passwords in plain text files in 2019[166]; and Amazon has severe data security shortfalls which routinely expose users' information to potential breaches, theft and exploitation.[167] Additionally, once a market has tipped to a sub-optimal privacy equilibrium, network effects make it very difficult for anyone to challenge this position.

In this environment self-correction is dubious, and non-intervention so far has actually resulted in stagnant and harmful digital markets and below-optimal levels of privacy and choice for users.[168] Consequently, not only is Article 102 TFEU intervention justified, but is positively warranted in such circumstances. This is in line with previous observations by the OFT and ex-DG Competition Director General Philip Lowe, who noted that in the context of exploitative abuses, '*we should continue to prosecute such practices where the abuse is not self-correcting*….'.[169]

False positives versus false negatives

Although traditionally underenforcement of antitrust has been viewed as preferable to overenforcement; recently, the contrary view appears to be more popular in context of digital

[165]Economides and Lioanis (n 74) 14-29.

[166]Whittaker, 'Researchers find 540 million Facebook user records on exposed servers' (*Techcrunch*, 3 April 2019) < https://techcrunch.com/2019/04/03/facebook-records-exposed-server/> accessed 30 May 2021.

[167]Manancourt, 'Millions of people's data is at risk' — Amazon insiders sound alarm over security' (*Politico*, 24 February 2021) <https://www.politico.eu/article/data-at-risk-amazon-security-threat/> accessed 28 May 2021.

[168]Stigler Report (n 25) 216.

[169]Lowe, 'How different is EU anti-trust? A route map for advisors' (Speech at ABA 2003 Fall Meeting, Brussels, 16 October 2003) < https://ec.europa.eu/competition/speeches/text/sp2003_038_en.pdf> accessed 28 May 2021.

markets.[170] This is particularly due to the unlikelihood of self-correction in such markets (discussed above), and the harmful implications of dominant firms' exploitative data-related conduct on economic welfare. Specifically, platforms' extensive and covert data harvesting techniques exacerbate information asymmetries and can result in increasing degrees of consumer exploitation.[171]

Unless there is a recalibration of competition law's tolerance for underenforcement, the market is likely to stagnate at such sub-optimal levels. This is particularly the case given platforms' incentive to increase their levels of data harvesting, the stickiness of data-opolies' market power, and additional user lock-in caused by dominant platforms' tendency to grow into digital ecosystems. If unchecked, this can result in significant harms to competition and consumer welfare, which can manifest in fewer choices, lower quality, degraded privacy and autonomy, higher prices and stunted innovation. For instance, the market is already functioning below-par when it comes to consumer privacy.

Therefore, unlike traditional markets, the prevalent view in the data economy is that false negatives could be costlier than false positives. Consequently, depending on the specifics of each case, abusive conducts in the data economy potentially warrant a more interventionist approach.[172]

[170]Cremer Report (n 16) 50; US HJR (n 26) 39; Stigler Report (n 25) 94.

[171]Ezrachi and Robertson (n 2) 1,4.

[172]Stigler Report (n 25) 94.

Impact on innovation

Remedies curbing exploitative data harvesting and aiming to promote privacy for users are unlikely to discourage innovation. On the contrary, they may enable a differentiation of business models followed by digital platforms and encourage privacy-protecting innovations.[173] Additionally, it is possible to devise remedies which tackle exploitative data harvesting without undermining platforms' incentives to invest and innovate. For instance, mandating firms to be transparent in how they collect user data and to obtain meaningful user consent (in line with the GDPR), is unlikely to have a chilling effect on platforms' incentive to innovate.

Market regulation risks and practical enforcement challenges

The remedies for excessive data extraction may be straightforward in most cases (example providing more choices to users), thereby obviating the risk of price/market regulation. Also, determining the appropriate benchmark for unfair data collection, example by reference to the GDPR, is much easier than determining when a price charged is excessive; and, can also address enforcement challenges prevalent in traditional markets (further discussed in Sections 5 and 6).[174]

Overall, the traditional objections against Article 102 TFEU intervention in exploitative abuse cases are less relevant in context of the data economy. Additionally, the CJEU appears to have adopted a de facto enforcement policy in excessive pricing cases, by intervening only

[173]Economides and Lioanis (n 74) 42.

[174]Terra Incognita (n 151) 88.

in situations characterized by two common criteria or filters - high and non-transitory entry barriers, and super-dominance.[175] Notably, these filters have also been adopted in relation to other exploitative conducts.[176] For instance, in *AKKA/LAA* the dominant company enjoyed a legal monopoly; and, in *United Brands* there was super-dominance due to high structural barriers, thus making market entry very unlikely. Additionally, the two sectors which have seen recent excessive pricing enforcement i.e., pharmaceuticals and energy, also share these characteristics.[177]

As already highlighted, these filters i.e., high entry barriers and super-dominance, are also very common in digital markets. For instance, online platforms might be super-dominant due to the large quantity of personal data they control, and high-barriers could be the result of direct and indirect network externalities. Therefore, the applicability of these filters in the data economy constitutes an additional justification for Article 102 TFEU intervention in cases involving exploitative data harvesting. And although there are some limitations to what Article 102 TFEU can achieve in this context, these can be effectively addressed (Section 7).

Having established the rationale for sanctioning exploitative abuses in the data economy, the next Section explores the feasibility of the first ToH introduced in Part 4.1; i.e., excessive data harvesting as an Article 102 TFEU violation.

[175]ibid 34.

[176]ibid.

[177]OECD, *Excessive Pricing in Pharmaceutical Markets - Note by the United Kingdom* (DAF/COMP/WD, 2018) 6<https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD(2018)110&docLanguage=En> accessed 28 May 2021.

5. EXCESSIVE DATA HARVESTING AS AN ARTICLE 102 TFEU VIOLATION

As mentioned in Section 4, a key ToH in tackling exploitative data harvesting is sanctioning '*excessive data collection as an Article 102 TFEU violation*'. The essence of this approach is that users' data is their counter-performance for otherwise free online services, and when an excessive amount of this counter-performance i.e., data is extracted from users; it is an exploitative abuse under Article 102(a) TFEU, similar to how extracting excessive prices is exploitative.

Under this ToH, excessiveness can be analysed using three different approaches. First, keeping strictly in line with an excessive pricing analogy, it is possible to view data-as-price and analyse if excessive data collection can be sanctioned like an excessive pricing abuse (Part 5.1). Second, the data harvested may be considered excessive if it is beyond what might be considered a fair exchange in light of the service provided (Part 5.2). Third, excessiveness could also be analyzed in reference to external benchmarks like the GDPR (Part 5.3).

5.1. EXCESSIVE DATA COLLECTION AS AN EXCESSIVE PRICING ABUSE

This Part explores the feasibility of viewing personal data as price and accordingly sanctioning excessive data collection as an excessive pricing abuse. In doing so, it first discusses the

monetary value of data, and then analyses traditional excessive pricing cases to identify potential benchmarks for excessiveness in the data economy.

The monetary value of data

In today's platform economy most online services are seemingly free. As such, envisaging an excessive pricing like abuse in this context might appear a bit counterintuitive, and one might ask – how can consumers pay too much while paying nothing?

The answer to this question is, consumers don't pay 'nothing' for these services - they pay with their data. The fact that personal data is the '*new currency of the Internet*'[178] has received increasing acceptance around the world. For instance, in the US, ex-FTC Chairwoman Ramirez noted how '*today's currency is data*'[179]; and in Europe, data's monetary value has been acknowledged by the EDPS[180] and in the 2018 European Electronic Communications Code.[181] Similarly, in a recent case against Facebook's data collection practices, an Italian Court noted how personal data can be considered a negotiable asset susceptible to economic exploitation, and considered a 'counter-performance' in a contract.[182] This new business model characterized by data as a means of payment in lieu of monetary

[178]Kanter, 'Antitrust Nominee in Europe Promises Scrutiny of Big Tech Companies' (*The New York Times*, 3 October 2014) <http://bits.blogs.nytimes.com/2014/10/03/antitrust-nominee-in-europe-promises-eye-on-big-tech-companies> accessed 28 May 2021.

[179]Wyatt, 'Edith Ramirez Is Raising the FTC's Voice' (*The New York Times*, 22 December 2014) < https://www.nytimes.com/2014/12/22/business/federal-trade-commission-raises-its-voice-under-its-soft-spoken-chairwoman.html> accessed 28 May 2021.

[180]2014 EDPS Opinion (n 83) 10.

[181]Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast) [2018] OJ L321/36, recital 16.

[182]OECD Data-Rights Report (n 31) 48.

compensation was also explicitly acknowledged by Commissioner Vestager, as per whom, consumers '*don't pay a single penny for those service*s', '[*i*]*nstead, they pay with their data'*.[183] Interestingly it has also been observed how zero payment in the data economy doesn't imply that the product is 'free' for the customer; it is just another point on the spectrum and a zero price is a deliberate number set by the profit-maximizing firm whilst imposing other costs (ex., attention and information costs) on users.[184]

Expressing data in monetary terms has a significant advantage from a competition law perspective. Antitrust tools were primarily developed for competition on price; and as noted in Section 3, this is particularly the case for exploitative abuses which have evolved around excessive pricing. Therefore, if dominant platforms' extensive data harvesting can be expressed and pursued in a similar way to excessive pricing abuses, such conduct can be sanctioned with minimal departure from the well-established Article 102 TFEU framework and competition economic tools.[185] This is one of the key benefits of this approach.

Also importantly, this data-as-price analogy appears to be practically feasible and economists are increasingly developing methodologies, for instance those based on market valuations, for calculating the value of personal information and ascribing a quantifiable price to data.[186]

[183]Vestager, 'Making Data Work For Us' (Data Ethics event on Data as Power, Copenhagen, 9 September 2016)<https://wayback.archive-it.org/12090/20191129211903/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-work-us_en> accessed 28 May 2021.

[184]Newman, 'Antitrust in zero-price markets: foundations' (2015) 164 University of Pennsylvania Law Review 149, 172 <https://scholarship.law.upenn.edu/penn_law_review/vol164/iss1/4> accessed 28 May 2021.

[185]Kerber, 'Digital markets, data, and privacy: Competition law, consumer law and data protection' (2016) 11 Journal of Intellectual Property Law & Practice 856, 860.

[186]Bania, 'The role of consumer data in the enforcement of EU competition law' (2018) 14(1) European Competition Journal 38, 66; OECD, 'Methodologies for Measuring Monetary Value' (2013) (n 17); Malgieri and Custers, 'Pricing Privacy – the Right to Know the Value of Your Personal Data' (2018) 34 Computer Law

However, despite the popularity and feasibility of viewing data as money, there exist some challenges to this approach which need to be addressed.

A key objection is that there are certain non-monetary values associated with data like privacy, dignity, autonomy and morality; and expressing personal data's value in monetary terms ignores this dimension.[187] Overlooking that excessive data harvesting also deprives individuals of such values (and not just data) is particularly problematic in the EU where privacy is a key fundamental right.[188]

Further, although the analogy broadly seems acceptable; there are various ways in which '*data is not like money'*[189] and has considerably different characteristics, for instance in respect of its imitability and lack of scarcity. Providing data to one platform, '*does not reduce the user's ability to provide the same data to…multiple other services*', which is '*a fundamental difference to excessive pricing cases where customers are left with less money/wealth once they have been exploited*.'[190] Therefore, legal provisions based on the grounds of monetary remuneration need substantial changes before they can be applied to data.[191]

Additionally, practical difficulties can also arise in agreeing on a data price – a relatively subjective notion. Specifically, data price can vary based not only on who is being

& Security Review 289, 296; Hoofnagle and Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price*'* (2014) 61 UCLA Law Review 606.

[187]Kerber (n 185) 857.

[188]Charter of Fundamental Rights of the European Union [2016] OJ C 202/389, art 8.

[189]Haucap, 'Data Protection and Antitrust: New Types of Abuse Cases? An Economist's view in light of the German Facebook Decision' (*CPI Antitrust Chronicle*, February 2019) 2.

[190]ibid.

[191]Robertson (n 34) 174.

asked[192], but even in respect of the same person, the value attached to one's own data and corresponding digital goods can be highly contextual and variable i.e., the super-endowment effect.[193] Another key issue here is determining whether data price should be ascertained as per the users' or the platform's valuation (both feasible approaches); with the latter being a potentially more objective approach given the super-endowment effect.

Finally, it is also sometimes difficult to draw the line between personal data as counter-performance; and, personal data that users provide in their own interest, for instance, to help improve the platform's quality.[194] Additionally, user payment through eyeballs or attention (in accepting an increasing amount of targeted advertising) also constitutes a price-like element, and so, may have to be factored into this analysis.[195]

There is substantial debate about each of the abovementioned challenges, exploring which in any further detail is outside the scope of this thesis. This discussion was primarily to highlight the essence of these objections, which must be kept in mind while discussing the data-as-price approach. Assuming these limitations can be addressed; the next step is determining the relevant benchmark for assessing excessiveness in the data economy.

[192]Kalimo and Mejcher, 'The concept of fairness: Linking EU competition and data protection law in the digital marketplace' (2017) 42 EL Review 210, 230.

[193]Winegar and Sunstein, 'How Much Is Data Privacy Worth? A Preliminary Investigation' (2019) 42 Journal of Consumer Policy 425, 430.

[194]Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' (2018) Max Planck Institute for Innovation and Competition Research Paper No. 18–23, 27.

[195]Robertson (n 34) 174.

The benchmark for an 'excessive' data price

The fact that consumers pay for online services with their data, '*doesn't have to be a problem, as long as people are happy that the data they share is a fair price to pay for the services they get in return'* (Commissioner Vestager).[196] However, in practice, the extent of data collection by dominant firms today is far from 'a fair price' paid by consumers, and has even been viewed as incentivizing a shadow economy based on unnecessary and insecure data processing.[197] Here, a key question is, at what point does the data collected stop being a fair price and becomes exploitative under Article 102 TFEU? That is, when does legitimate data collection stop and excessive data collection begin?

Under the data-as-price approach, this can be answered by analysing if the concerned data collection conduct fulfills the criteria for establishing an excessive pricing abuse. As discussed in Section 3, the seminal test here is that set out in *United Brands* (UB), with the option of also using *other ways* where required. For analysing excessiveness in the data economy, it is appropriate to use such a combined approach – with the UB test providing the critical reference point, while also incorporating comparative benchmarks. The application of the specific UB steps in the data economy i.e., determining (i) the excessive nature of the price compared to the economic value of the product and (ii) the unfair character of the price; is further discussed below.

[196]Vestager speech (n 183).

[197]Submission from Ryan (Brave) and Lynskey on Competition issues in digital markets to the CMA (7 October 2019) para 24 < https://assets.publishing.service.gov.uk/media/5d6e247a40f0b6092247e3e4/190730_Brave_and_Lynksey__LSE__-_Response_to_SoS_-_non-confidential.pdf> accessed 24 June 2021.

1. *UB test – Step 1*

The first stage of the UB test entails performing cost-price comparisons to analyze the excessiveness of price compared to the product's economic value.[198]

As noted by Robertson, after expressing data in monetary terms, here the next step is to analyse the price paid by the user i.e., amount of personal data gathered by the dominant platform through tracking; and second, what the user receives in return i.e., the product's cost to the service provider and its economic value.[199] The next stage is ascertaining if there is a reasonable relationship between the amount of data collected and the economic value of the digital service users receive.[200]

As illustrated by Bostoen's analysis of Facebook, although theoretically possible, there are various complexities in this assessment.[201] In his analysis, juxtaposing the price of Facebook per year (i.e., Facebook's average revenue per user/the value Facebook derives per user's data), with its value per month (a complex assessment, broadly ascertained by surveying users' willingness-to-pay for Facebook); indicated that Facebook users were indeed getting value for their money (data).[202] As such, prima facie, there appeared to be a reasonable relation between the amount of data collected and economic value of service received. But some important factors rendered such analysis incomplete. Specifically, users are often not in a position to assess the overall value of services received and data divulged;

[198]UB (n 1212) para 252.

[199]Robertson (n 34) 175.

[200]ibid.

[201]Bostoen, 'Online Platforms and Pricing: Adapting Abuse of Dominance Assessments to the Economic Reality of Free Products' (2019) 35(3) Computer Law & Security Review 263, 278-279.

[202]ibid.

for instance, because they are unaware of the extent of their counter-performance or third-party tracking[203], they underestimate the value of their personal data etc.[204] Also, the platform's current revenue may not be a reliable indicator of future data value, thus further complicating this analysis.[205] Additionally, the concept of 'reasonability' can be quite vague as a legal benchmark, especially when assessed in qualitative (rather than quantitative) terms.

Consequently, there exist some challenges in determining a clear criterion for excessiveness and what an ideal ratio between data collection costs and price should be.[206] Such ambiguity indicates a definite requirement for better analytical tools in applying the first step of the UB test in the data economy.[207]

2. *UB test – Step 2*

The second stage of the UB test entails analyzing the *unfairness* of price - either '*in itself or when compared to competing products'*.[208] In the platform economy this entails determining if the amount of data collected is excessive - in relative or absolute terms.[209]

[203]Ezrachi and Robertson (n 2) 10.

[204]Newman, 'The costs of lost privacy: Consumer harm and rising economic inequality in the age of Google' (2014) 40 William Mitchell Law Review 849, 857.

[205]OECD AoD (n 121) 50.

[206]Kalimo and Mejcher (n 192) 231.

[207]OECD AoD (n 121) 50.

[208]UB (n 122) para 252.

[209]Robertson (n 34) 175.

In determining *relative* excessiveness, a comparative approach is feasible and the concerned price can be compared to those charged for identical services elsewhere; provided that these reference transactions are selected '*in accordance with objective, appropriate and verifiable criteria'*.[210] Applying this test in the data economy is, however, challenging; particularly, due to the difficulty in identifying suitable reference transactions. Given how the tracking environment is dominated by just a few data-opolies, there is an absence of effective competition, making it difficult to know what a competitive level of consumer data sharing would be. This is aggravated by the fact that existing platforms have very similar terms of service when it comes to user data.[211] Additionally, comparing the prices of 'free' services across online platforms could be quite complex, particularly as the existence of double-sided platforms implies that a competing product on one side may not constitute a competing product on the other side.[212] Therefore, a benchmark which looks at privacy policies in different markets may not be very helpful.

However, a comparison of the platform's own data collection practices over time could be a suitable approach. This entails tracing changes in the tracker's own privacy policies to determine if a given policy is excessive, for instance, when an increase/decrease in the platform's data collection corresponds to a new market entry/exit.[213] The steady deterioration in Facebook's privacy policy which corresponded to its steady increase in

[210]*AKKA/LAA* (n 147), para 41.

[211]Davilla, 'Is big data a different kind of animal? The treatment of big data under the EU competition rules' (2017) 8 JECLAP 370, 381.

[212]Terra Incognita (n 151) 75; Robertson (n 34) 176.

[213]Robertson (n 34) 176.

market power[214], is an illustrative example of the same. However, this analysis would also have to account for the platforms' evolving technologies/services, and if these warrant more data collection.[215]

Additionally, as per the CJEU in *AKKA/LAA*, to be appreciable such disparity in prices (i.e., differences in amount of data collected) must be significant and persistent[216]; both vague terms, leaving a broad margin of discretion and a high risk of decisions being annulled by higher courts. For instance, in the recent pharmaceutical sector decisions, there was significant variation in the threshold at which price increases were considered unfair; with the lowest threshold being a 300% price increase in the *Italian Aspen* case, and the highest being a 2600% price increase in *Pfizer/Flynn*. Such uncertainty is even more problematic in the data economy, where online platforms' vague privacy policies can constitute a prima facie obstacle to comparison.

In addition to the abovementioned relative approach, it is also possible to analyse excessiveness in *absolute* terms. This entails specifying what an undue or unreasonable collection of data connotes[217], which can be done using external benchmarks (ex., the GDPR) as normative yardsticks.[218] The nuances of relying on such external benchmarks are further discussed in Part 5.3.

[214]Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy' (2019) 16 Berkley Business Law Journal 39.

[215]Robertson (n 34) 176.

[216]*AKKA/LAA* (n 147), para 55.

[217]Robertson (n 34) 177.

[218]Costa-Cabral and Lynskey (n 67).

Therefore, although it is theoretically plausible to express data-as-price and accordingly satisfy the analytical requirements of the two-step UB test (albeit with some tweaks); this approach entails a high standard of proof, and there are various challenges in defining a clear-cut threshold for applying these tests. Against this backdrop, no competition authority has ever sanctioned any case of excessive pricing in a data market; and even the BkM - a pioneer in sanctioning exploitative abuses in the digital economy - steered clear of this approach in the Facebook case.

However, instead of viewing 'data-as-price' and then establishing excessiveness; another approach where data is viewed as the focal point and the benchmark for excessiveness is what the service requires is also possible.

5.2. EXCESSIVENESS AND FAIRNESS OF DATA COLLECTION RELATIVE TO THE SERVICE

An alternative to the data-as-price approach, is to analyse if the data harvested is beyond what might be considered a fair exchange in light of the service provided.

Here, data is not converted into price; but instead, data itself is the focal point to assess excessiveness. As such, the essence of this approach is examining the volume and scope of data needed for the service - which is the key benchmark here, comparing it with how much extra data was actually harvested, and then analysing if this gap is 'excessive'. Notably, the EDPS has also observed how exploitative abuses may occur if '*the "price" paid through the*

surrender of personal information [is] to be considered excessive in relation to the value of the service consumed... '.[219]

A significant advantage here is that the many challenges associated with expressing data in monetary terms and then applying the excessive pricing/UB framework to the same, don't apply to this approach. For instance, as the relevant benchmark here is what is required for the service, complications arising from whose perspective to account for when considering data excessiveness – the user's or the platform's – are irrelevant. Similarly, concerns regarding users not fully understanding the extent of their counter-performance also don't apply. Therefore, this approach entails fewer complications than the previously discussed data-as-price method.

However, data excessiveness benchmarked against what is required to offer the service, also has its own set of open-ended questions and complexities. For instance, is the benchmark centered around the minimum amount of data needed to operate the service? Or should it be based on the profit expected, or motive to innovate? Additionally, online platforms ordinarily operate in double-sided markets where the contours of the services provided are not static or easily discernable, with some degree of personalization and targeted advertising being increasingly viewed as welfare-enhancing and an intrinsic part of such services. Example, Instagram users expect to see relevant content in their feed, and dislike junk advertising. Consequently, it is often tricky to draw the line between service-related data harvesting and excessive data harvesting. Additionally, platforms can also justify increased data collection on the premise that it is being used for improving product quality (example

[219]2014 EDPS Opinion (n 83) 29.

better search results/targeted advertising); a defence which was used by Facebook before the BkM.

Interestingly, the BkM rejected such a broad justification. It distinguished between user data directly collected on the Facebook platform and data acquired from other external sources; emphasizing that only the former was necessary for Facebook.[220] As such one way of drawing the line between justified and exploitative data collection, could be to distinguish between data collected through authorized first-party tracking versus data harvested through third-party tracking and in stealth mode. Further, as observed by Haucap, data extraction may be considered excessive '*once we assume that (a) either a sufficient number of consumers do actually receive disutility from 'excessive' data requirements and from having their data combined or (b) consumers are somehow being harmed without noticing it'*.[221]

Additionally, given that this approach analyses whether the data harvested is a *fair* exchange in light of the service provided, whilst going beyond the realm of pricing; here, reliance could also be placed on the notion of '*other unfair trading conditions*' in Article 102(a) TFEU, to ascertain the exact threshold for excessiveness. Data is ordinarily harvested on the basis of contractual terms or privacy policies, which are therefore, relevant as trading conditions under Article 102(a).[222] This creates an avenue for exploring if excessive data

[220]Witt (n 120) 23.

[221]Haucap (n 189) 3.

[222]Schneider, 'Testing Art.102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's investigation against Facebook' (2018) 9(4) Journal of European Competition Law & Practice 213, 221.

collection by dominant platforms, relative to what is required for the service and as imposed on users through the firms' privacy policies, could constitute an unfair trading condition.

Notably, a majority of firms have misleading and opaque privacy policies with terms which are unclear, difficult to understand, lengthy, constantly changing and so vague that their consequences are difficult to comprehend and foresee; which are then leveraged by platforms to extract unfair amounts of data from users. Here, existing Article 102(a) TFEU jurisprudence could be used to ascertain the precise threshold at which such trading conditions, i.e., privacy policies, can be considered unfair (and the data collected, viewed as excessive in relation to the service).

Unfair trading conditions have been previously addressed by the CJEU and EC in a few cases, based on which some specific criteria can be inferred. At a preliminary level, Courts have primarily considered unilaterally imposed clauses abusive, rather than extensively negotiated terms[223]; a criterion which is fulfilled by non-negotiable privacy policies imposed on users by dominant platforms. Such unilaterally imposed clauses have then been considered unfair in a variety of circumstances. In *SABAM*[224], the CJEU found that the imposition of obligations which are not necessary for the attainment of the object would be in breach of Article 102(a). This test was interpreted by the Commission in *GEMA statutes* as requiring indispensability (i.e., absolutely necessity) and equity (i.e., not unnecessarily limiting the freedom of the parties).[225] The Commission also stressed the importance of these conditions in *Tetra Pak II*, where the obligations in casu '*ha[d] no connection with the purpose of the*

[223]Terra incognita (n 151) 18.

[224]*BRT v Sabam* (n 158).

[225]*GEMA statutes* (Case IV/29.971) Commission Decision 82/204/EEC [1981] OJ L94/12, para 36.

contract'.[226] Thereafter, in *DSD* the Commission highlighted the relevance of the proportionality principle, which entails analysing the bargaining power between contractual parties; and in which context, take-it-or-leave-it clauses were held to be disproportionate and so, 'unfair'.[227]

Based on such case-law, key parameters for assessing the unfairness of trading conditions are the principles of indispensability, equity and proportionality; the parties' respective bargaining power; and, the dominant company's operational interest and transparency involved in imposing the conditions.[228]

These tests can be applied in the digital economy as follows: In respect of the *indispensability test,* it would have to be determined if the data harvesting conditions are absolutely necessary in light of the purpose of the agreement between the platform and user. The multi-sidedness of most digital platforms may complicate this analysis. For instance, if the monetization of user data (for example, through targeted advertising) is regarded as the key objective, then collecting larger amounts of data would be justified; however, if the provision of a digital service (for example, social media) is understood as the agreement's primary objective, then 'indispensable' data would be limited to only that data which is required to run the service profitably.[229] The purpose of data collection could also be for a combination of these two objectives. As mentioned above, a potential way of addressing this

[226]*Tetra Pak II* (Case IV/31043) Commission Decision 92/163/EEC [1991] OJ L72/1, para 107.

[227]*DSD* (n 156), para 112.

[228]Colangelo and Maggiolino, 'Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the US' (2018) 8(3) International Data Privacy Law 224; Robertson (n 34) 181.

[229]Robertson (n 34) 180.

issue is distinguishing between data collected on the platform and data accumulated through unauthorized third-party tracking. As per the *equity test,* the firm's privacy policies (and so, data collection) would be required to not unfairly limit users' right to privacy.[230] As copyright laws did in *SABAM* and *GEMA statutes*, data protection legislations can provide a useful reference point in ascertaining what unfairly limits privacy rights. The *proportionality principle* entails considering the asymmetry in bargaining powers of trackers and users, and weighing the amount of data divulged by users against the benefits they obtain from the digital platform; and importantly, also accounts for situations where take-it-or-leave-it terms are unilaterally imposed by dominant platforms. [231]

In accordance with the above, we see that the analytical framework set out in the unfair trading conditions jurisprudence under Article 102(a) TFEU is capable of being applied to the data economy, and can provide further support in analysing when data collection is excessive in relation to the service provided. This approach is relatively less challenging than the data-as-price approach in Part 5.1; and can be especially useful where the level of data collected, especially through third-party tracking, is clearly excessive in relation to the service provided.

However, it does entail some uncertainty and a key objection here is that it can excessively broaden the scope of Article 102 TFEU. It also offers significant policy discretion to competition authorities, thereby '*inject[ing] an undesirable level of discretion*' in how this

[230]ibid.

[231]ibid 181.

legal category is interpreted.[232] The fact that this approach can be '*more art than science*'[233] also increases the chances of any related decisions being overturned on appeal, which could discourage competition authorities from pursuing enforcement. Notably, this ambiguity can potentially be addressed by drawing normative guidance from relevant external benchmarks within the EU legal family, example, the GDPR or consumer laws. For instance, a finding that the data being collected is not indispensable to the provision of the service can be supported by the GDPR's data minimization and purpose limitation principles (Articles 5(1)(b) and (c) respectively). Such references to wider EU legislations are further discussed below.

5.3. EXCESSIVENESS IN RELATION TO EXTERNAL BENCHMARKS

The two approaches discussed so far demonstrate how EU competition law may already possess the tools to apply Article 102 TFEU to excessive data collection. However, their inherent limitations and complexities – particularly the absence of any credible thresholds – makes their practical enforcement challenging. To address such concerns, competition enforcers could rely on external legal frameworks like data protection laws to provide relevant thresholds. As noted by Lynskey, '[*d]ata protection law may play its biggest role as a normative yardstick under Article 102 TFEU*'.[234] Such an external benchmark serves two potential purposes:

[232]Cooper, 'Privacy and antitrust: Underpants Gnomes, the First Amendment, and subjectivity' (2013) 20(4) George Mason Law Review 1129, 1135.

[233]Donoghue and Padilla (n 131), 856.

[234]Costa-Cabral and Lynskey (n 67) 18.

First, it can support the above-mentioned approaches. In the data-as-price approach (Part 5.1), data protection legislations can be relied upon to assess absolute excessiveness. And under the approach in Part 5.2, such benchmarks can strengthen the unfairness assessment and resolve uncertainties in identifying when the data extracted is excessive in relation to the service provided.

Second, such external benchmarks could also constitute an independent approach in assessing when excessive data collection is abusive. Here, an infringement of rights granted by data protection law would provide a clear negative normative marker for such situations to be considered censurable from an antitrust perspective (provided that other competition law requirements are also met). By way of illustration, if a dominant platform extracts personal data beyond what is necessary to achieve a particular purpose or keeps it for a period longer than necessary, thereby breaching GDPR Articles 5(1)(b) and(c) (on data minimization and purpose limitation); this would be determinative of abusively excessive data collection under antitrust law, provided other Article 102 TFEU conditions, like dominance, are met. No additional steps – as was the case in Parts 5.1 and 5.2 – would be required. This reliance on external benchmarks as an independent threshold for sanctioning excessive data collection constitutes the third approach under this ToH. And given that it is certain and free from the myriad enforcement challenges underlying the previous approaches, it has higher chances of practical implementation.

Therefore, this third 'external benchmarks' approach is arguably superior to the approaches in Parts 5.1 and 5.2, which only rely on the GDPR for added certainty.

Such reliance on external legislative frameworks is justified and appropriate, particularly given how European competition law has traditionally always been open to other

areas of law for normative context; for instance, intellectual property law and national law have provided the relevant 'normative backdrop' for several antitrust cases.[235] Additionally in *AstraZeneca*, a case pertaining to the provision of misleading information by a dominant undertaking, the CJEU explicitly recognized that the breach of another area of law can be a factor in deciding if there has been a violation of competition law as well.[236] Notably in the Facebook case, the BkM used GDPR Article 6 as a benchmark for determining that Facebook's business terms were exploitative. And although this decision was based on German law, a similar approach is also justified at the EU level; as explicitly acknowledged by distinguished Judge Thomas von Danwitz (president of the 4th chamber of the CJEU).[237] He noted how the German Facebook case and similar circumstances covered by the GDPR (ex., inadequate user consent, lack of choice re privacy etc.) fall neatly into the line of cases like *Sabam, AstraZeneca, Der Grüne Punkt* or *Allianz Hungaria* [238] Previously, the President of the French competition authority also declared that EU privacy rules were '*key to competition analyses*'[239]; and in a 2012 speech, then EC Commissioner Almunia affirmed that in the future the Commission may look at cases where a dominant company abuses its position

[235]Robertson (n 34) 182; Costa-Cabral and Lynskey (n 67) 27.

[236]Case C-457/10P, *AstraZeneca v. Commission*, EU:C:2012:770; Robertson (n 34) 182; Kalimo and Mejcher (n 192) 226.

[237]Thomas von Danwitz (*19th International Conference on Competition in Berlin (IKK*), 15 March 2019) reported by Rupprecht Podszun' <www.d-kart.de/blog/2019/03/15/conferencedebriefing-7-international-competition-conference-berlin/> accessed 28 May 2021.

[238]ibid.

[239]Gladicheva 'EU privacy rules key to competition analyses, head of France antitrust watchdog says' (*GCR Live: 7th Annual Telecoms, Media & Technology*, 4 May 2018).

by infringing privacy laws.[240] Similar observations were also made in the French-German Report[241] and 2014 EDPS Opinion[242]. This argument garners additional support from the fact that both EU data protection and competition laws are underpinned by notions of fairness.[243]

Therefore, resorting to data protection legislations – which are meant to identify the contours of legitimate data collection – to provide normative context to what an undue or unreasonable harvesting of data connotes under antitrust law[244], is completely justified.

Admittedly, this threshold has some limitations. First, it targets only those conducts which entail an excessive collection of data and unequivocally infringe the GDPR, with the rest flying under the radar. However, this is preferable to the current situation where no act of excessive data collection, regardless of how exploitative it is, is caught under Article 102 TFEU. Second, there also exist some arguments to the effect that such an approach instrumentalizes antitrust to achieve the aims of data protection law. Although that is not the case here, as the GDPR is only providing competition law with a normative framework in the absence of the price parameter; given the traditionally purist attitude towards antitrust, this instrumentalization argument cannot be completely ignored (even if one disagrees with it). However, there exists an alternate ToH where competition law can rely on such benchmarks without raising this instrumentalization objection, and is discussed in the next Section.

[240]Almunia, 'Competition and personal data protection' (Privacy Platform event: Competition and Privacy in Markets of Data, Brussels, 26 November 2012) < https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860> accessed 28 May 2021.

[241]French-German Report n(10) 25.

[242]2014 EDPS Opinion n(83)15.

[243]Graef et al, 'Fairness and Enforcement: bridging Competition, Data Protection and Consumer Law' (2018) 8(3) International Data Privacy Law 200.

[244]Gebicka and Heinemann, 'Social Media & Competition Law' (2014) 37(2) World Competition 149, 165.

Finally, similar to data protection legislations, consumer laws like the UCPD, UCTD and the recent EU Platform-to-Business (P2B) regulation[245] could also serve as external benchmarks; particularly in relation to misleading or deceptive privacy policies.[246] For instance, in determining at what point a (change in) privacy policy should constitute an exploitative abuse under Article 102(a) TFEU, UCPD Article 6(1) on misleading commercial practices may be of assistance.[247]

Therefore, EU competition law is already equipped with the required tools to target excessive data collection under Article 102 TFEU, especially under the third external benchmarks approach. However, given the drawbacks of relying just on the GDPR to prove an antitrust infringement, there is some scope for a more robust ToH. Specifically, it would be useful to have an approach which (i) can incorporate data protections legislation into the internal logic of antitrust law thereby avoiding the instrumentalization argument, and (ii) target a broader range of exploitative data harvesting conducts. In this context it would be useful to look at the next Section which discusses the second ToH, i.e., a privacy-quality degradation constituting an exploitative abuse of dominance.

[245]Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57.

[246]Robertson (n 34) 177.

[247]Graef (n 243) 213.

6. DEGRADATION OF PRIVACY – QUALITY AS AN EXPLOITATIVE ABUSE

The previous Section looked at excessive data harvesting as an Article 102 TFEU violation using three distinct approaches. And although these were all theoretically possible (to varying degrees), they suffered from some limitations – especially from a practical enforcement perspective – thus creating room for an alternate ToH.

This Section analyses exploitative data harvesting through a new lens - specifically, whether a degradation of user privacy (caused by data harvesting) could be viewed as a degradation in the product/service quality, thereby constituting an exploitative abuse of dominance under Article 102(a) TFEU.

Here, Part 6.1 discusses the significance of quality as a competitive parameter and how privacy could constitute a dimension of quality. Part 6.2 explores the various privacy-degrading conducts which could be sanctioned under this ToH. Part 6.3 discusses the two key challenges to this approach – difficulties in assessing (i) 'quality' as a competitive parameter, and (ii) privacy as a dimension of quality. Thereafter Part 6.4 discusses potential ways of resolving these challenges, and Part 6.5 explores how using an additional threshold (example, the GDPR) could make this ToH more practically feasible.

6.1. PRIVACY AS A DIMENSION OF QUALITY

This Part establishes the building blocks to this ToH. First it elaborates upon the significance of 'quality' as a competitive parameter, and then establishes how privacy can be a dimension of product/service quality.

Quality as a parameter of competition

As highlighted previously, historically competition law enforcement has primarily focused on pricing. However, in addition to price, there exist other parameters which determine whether consumers will buy a particular product or service, and which firms often compete over; namely quality, choice and innovation.[248] For instance, in *Microsoft/Skype* the ECJ emphasized on parameters like innovation and service quality[249]; and recently, in *Dow Chemical/DuPont* the Commission focused extensively on the concentration's effect on innovation.[250]

This Section focuses on the quality criterion, a key non-price consideration that determines whether consumers will purchase a product; and which in the long run, also fosters innovation and economic growth.[251] It is widely acknowledged that competition policy is concerned as much with quality as it is with price, and conducts that negatively affect quality

[248]Case C-209/10 *Post Danmark A/S v Konkurrencerådet* [2012] ECR 2012 -00000, para 22; Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2004] OJ C-101/97, para 8; Guidelines Article 82 (n 62) para 5; Antitrust Division of the US Department of Justice, Horizontal Merger Guidelines 2010, para 2.

[249]*Microsoft/Skype* (Case COMP/M.6281) Commission Decision C 7279 [2011] OJ C-341.

[250]*Dow/DuPont* (Case COMP/M.7932) Commission Decision (2017) 1946 final.

[251]OECD Quality Report (n 160) 22.

are equally harmful to consumer welfare as output reductions and price increases (if not more harmful, example in cases involving safety standards for consumer goods).[252]

Traditionally however, antitrust enforcers have avoided relying solely on the quality criterion; using price considerations to account for quality aspects instead, example decreased quality being reflected in lower prices. But this reliance on price to cater for quality aspects, in other words the heuristic '*you get what you pay fo*r', starts breaking down when the product/service is offered for free.[253] Consequently, in zero-price markets quality by itself becomes the primary measure of a firm's conduct or the '*relevant locus of competition'* (Valletti).[254] Similarly as per the Commission, where products are mainly offered for free consumers '*pay more attention to other features*', and quality '*is therefore a significant parameter of competition'*.[255]

Quality is multi-dimensional and often comprises of several attributes of a product. In the zero-price data economy, these dimensions include privacy and data security, functioning of web search engines, advertising content, ease of switching etc.[256] This Section focuses specifically on 'privacy' as a dimension of product-quality.

[252]Ezrachi and Stucke, 'The Curious Case' (n 160) 228, 229.

[253]ibid 232.

[254]Valletti (n 15) 4.

[255]*Microsoft/Yahoo! Search Business* (Case M.5727) [2010] Commission Decision of 18/02/2010, para 101; *Microsoft/Skype* (n 249) 81.

[256]OECD, *Quality considerations in digital zero-price markets* (Background Note DAF/COMP(2018)14) 10-22.

Privacy as a dimension of quality

In today's data economy, personal data harvesting and privacy considerations are part of the bargain when consumers use online services. Therefore, data protection conditions offered to individuals can reflect competitive parameters, particularly quality; and, the level of privacy offered by platforms can influence consumer decision-making.[257] As noted by Commissioner Vestager, '*every little thing that makes your service more appealing to consumers can help you to compete. And that includes better protection for personal data'*.[258]

In this background it has been argued that a loss of privacy may be viewed as a '*reduction in the quality of a good or service*'.[259] This was first acknowledged in 2007 at the time of the *Google/DoubleClick* merger, where Peter Swire observed how the combination of Google's '*deep*' information, with DoubleClick's '*broad*' information about the same users on other sites '*may [constitute]a significant reduction in the quality of the search product…'*.[260] The final FTC decision also somewhat acknowledged that mergers can '*adversely affect non-price attributes of competition, such as consumer privacy*'; however, this wasn't further accounted for in the judgment.[261]

[257]Costa-Cabral and Lynskey (n 67) 13.

[258]Esayas (n 85) 184.

[259]Swire, 'Protecting Consumers: Privacy Matters in Antitrust Analysis' (*Center for American Progress*, 19 October 2007) < https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/ > accessed 30 May 2021; 2014 EDPS Opinion (n 83) 13.

[260]ibid.

[261]*Google/DoubleClick* (n 95) 2-3.

This argument has now gained increased acceptance.[262] It was acknowledged by the EC in *Microsoft/LinkedIn*, and Commissioner Vestager has also explicitly noted that the Commission '*has ... integrated, where appropriate, data protection as a quality parameter*….'.[263] Similarly, Makan Delrahim (Assistant Attorney General of the US Justice Department's Antitrust Division) observed that since privacy is a dimension of quality, protecting competition '*can have an impact on privacy and data protection*'.[264] And, as per Maureen Ohlhausen (former Acting Chair of the FTC), quality reductions online could '*include factors such as….lessened control over privacy'*.[265] Recently, in complaints against Facebook in the US it was noted how Facebook harmed competition and '*the quality and variety of privacy options available to users of Personal Social Networking Services have been degraded, including but not limited to options associated with data gathering and data*

[262]Esayas, 'Privacy-As-A-Quality Parameter: Some Reflections on the Scepticism' (2017) Stockholm University Research Paper No. 43; Ezrachi and Robertson (n 2) 8; Stucke, Data-opolies (n 27) 285.

[263]Data and Privacy Hearing, 'Statement by Margrethe Vestager, European Commissioner for Competition' (*House Judiciary Committee - Subcommittee on Antitrust, Commercial, and Administrative Law*, 6 September 2019) 4 <https://docs.house.gov/meetings/JU/JU05/20191018/110098/HHRG-116-JU05-20191018-SD002.pdf> accessed 30 May 2021.

[264]Competition Policy and Consumer Rights on Oversight of the Enforcement of the Antitrust Laws, 'Statement of Assistant Attorney General Makan Delrahim' (*U.S. Senate Subcommittee on Antitrust*, 17 September 2019) <https://www.justice.gov/opa/speech/statement-assistant-attorney-general-makan-delrahim-us-senate-subcommittee-antitrust> accessed 30 May 2021.

[265]Ohlhausen, 'Online Platforms and Market Power Part 2: Innovation and Entrepreneurship hearing' (16 July 2019) 4 <https://www.bakerbotts.com/thought-leadership/publications/2019/july/online-platforms-and-market-power> accessed 30 May 2021.

usage practices.'[266] The notion of privacy-quality has also been stressed upon in the Furman report[267], Stigler Report[268] US HJR[269] etc.

Therefore today, there is an increasing recognition of the fact that privacy can constitute a dimension of product quality.

Importantly, it is dominant platforms' concentrated market power in the data economy which allows them to degrade privacy-quality for users. For instance, Facebook's approach to user privacy has changed drastically with an increase in its market power, and, '*in the absence of competition, [its] quality has deteriorated over time, resulting in worse privacy protections for its users….*'.[270] Specifically, when the social media market was competitive Facebook was very responsive to consumer privacy preferences and used privacy as a key factor to compete. It would routinely implement privacy-enhancing measures (ex., providing opt-out options from third-party tracking), withdraw tracking products (ex., advertising product Beacon), allow consumers to vote on future contractual privacy changes etc.[271] Similarly, in respect of potential acquisitions (ex., its purchase of Atlas in 2013), *'[m]anaging perceptions around privacy*' used to be an area of concern for Facebook.[272] However, once Facebook consolidated its dominant position and users had no other choice, it permanently changed its privacy policy

[266]*State of New York et al v Facebook,* Case 1:20-cv-03589-JEB Document 4 Filed 12/09/20, para 248; *See also FTC v Facebook,* Case 1:20-cv-03590-JEB Document 51 Filed 01/13/2 paras 42, 163.

[267]Furman Report (n19) para 1.128.

[268]Stigler Report (n25) 66.

[269]US HJR (n 26)18.

[270]ibid 14.

[271]Srinivasan, 'Case Against Facebook' (n 214).

[272]US HJR (n 26) 173.

towards a more active user tracking. In fact, in 2019 Facebook's lawyers argued that users had '*no privacy interest'*, because by the sheer act of using the platform they had '*negated any reasonable expectation of privacy*'.[273]

Therefore, dominant platforms can use their market power to deliberately reduce user privacy and so product/service quality, thus warranting Article 102 TFEU intervention. This is similar to how arbitrary price increases can constitute an exploitative abuse of dominance; and, has been considered to be a '*necessary adaptation'* of Article 102(a) TFEU in the context of data-driven ecosystems.[274] Additionally, such privacy-quality degradation can be caused through various practices.

6.2. PRIVACY-DEGRADING PRACTICES

In today's data economy where platforms' business models depend on harvesting, exploiting and monetizing personal data, market incentives run almost entirely in the direction of reducing user control over data[275]; which can be done using various mechanisms.

A significant way is harvesting and storing an excessive amount of personal data, example through amalgamation of multi-sourced data, data harvesting in stealth mode and with limited user awareness etc.

[273]Biddle, 'In Court, Facebook Blames Users For Destroying Their Own Right To Privacy' (*The Intercept*, 14 June 2019) < https://theintercept.com/2019/06/14/facebook-privacy-policy-court/ > accessed 5 June 2021.

[274]Robertson (n 34) 178.

[275]Stucke, 'Data-opolies' (n 27) 295.

Firms can also degrade privacy and reduce transparency through misleading and opaque privacy policies; previously also acknowledged as a potential abuse of dominance by EDPS Supervisor Buttarelli.[276] Online platforms' privacy terms are often vague and lengthy with unforeseeable consequences, thus rendering user consent in most cases insufficient and largely uninformed. For instance, privacy policies that an average internet user encounters every day could take approximately 250 hours per year to read.[277] As noted by the OECD, '*by keeping privacy policies deliberately vague, service providers make it difficult for consumers to evaluate the real value of their data*'.[278] With the rise in IOT's requiring default or adapted consent mechanisms, this scenario will only get worse.

Additionally, if a platform updates its privacy terms users *have* to agree to the same given their lock-in and high switching costs involved. As they don't have the same options they did the first time they used the platform, this is no longer a free choice.[279] Moreover, platforms routinely deviate from their initial data-use policy, which often goes undetected and is '*relegated to investigative journalists to discover and explain'*.[280] Also, dominant platforms often impose privacy terms and conditions on a take-it-or-leave-it basis, and given the lack of alternative options otherwise, users often have no choice but to accept such terms.

[276]Buttarelli, 'Keynote Speech' (Joint ERAEDPS Seminar on Competition Rebooted: Enforcement and personal data in digital markets, Brussels, 24 September 2015) <https://edps.europa.eu/data-protection/our-work/publications/speeches/competition-rebooted-enforcement-and-personal-data_en> accessed 30 May 2021.

[277]McDonald and Cranor, 'The Cost Of Reading Privacy Policies' (2008) 4(3) I/S: A Journal of Law and Policy for the Information Society 543.

[278]OECD 'Big Data' (n 159) 25.

[279]Stigler Report (n 25) 54.

[280]US HJR (n 26) 54.

To increase their control over data, platforms are also deploying manipulative interfaces and deliberately making it harder for users to navigate their privacy preferences (as highlighted in Section 1). Additionally, to prevent anyone from '*limiting their extremely valuable information collection*'[281] data-opolies often impose costs on companies seeking to promote privacy interests; example Google kicking the privacy app Disconnect out of its Android app store.[282]

Further, surveillance and security risks can significantly reduce user control over data. This includes identity theft, data loss, nuisance contracts and inadequate data security (ex., Facebook's eagerness to get third-party apps connected to its network led to mass data leaks[283]).[284]

Therefore, there is an increasing information asymmetry and a clear violation of user privacy and autonomy due to dominant platforms' market power and their use of exploitative techniques; thereby warranting antitrust intervention. However, there are some challenges to this privacy-quality ToH, example linking privacy degradations to a workable benchmark of quality; as further discussed below.

[281]US HJR (n 26) 48.

[282]Ezrachi and Stucke, *Virtual Competition* (n 59) chapter 16.

[283]Whittaker (n 166).

[284]CMA, *The commercial use of consumer data* (Report on the CMA's call for information, June 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf > accessed 30 May 2021.

6.3. KEY CHALLENGES

Although it is widely acknowledged that privacy can be viewed as a dimension of quality, there are two key challenges to measuring privacy as a quality-component of competition. First, measuring quality as a competitive parameter is tricky, and such traditional obstacles can also be expected in the data economy; and second, measuring privacy as a dimension of quality can be particularly complex due to the Privacy Paradox.

Measuring the 'quality' parameter

Quality is multidimensional, with both objective and subjective components; and as a competitive parameter, it has always been an elusive target for antitrust authorities.

The quality of a product incorporates wider criteria (depending on the product: speed, efficiency, etc.), all of which work together to influence the overall perception of product quality. Therefore, a deterioration of one criterion can be balanced by an improvement in another, with the overall perceived quality remaining the same. Consequently, a degradation of privacy-quality can be balanced by enhancing other dimensions of product quality; example, the additional data collected being used to provide welfare-enhancing personalization features like better search results, improved advertising etc. Therefore, it is possible for platforms to offer consumers a superior quality product overall, despite a degradation in privacy. Additionally, quality is a relative and highly subjective concept, and often what one person desires another can dismiss or revile; thus injecting further uncertainty into this analysis.

A deterioration of quality can also be balanced by improvements to other competitive parameters like price and innovation, thereby raising the question of whether one can offset

the other and to what extent. For instance, given that extensive data collection does allow platforms to provide lower/zero priced goods and services (which is valued by users), it can be argued that a degradation of privacy-quality is offset by an improvement in price.[285] Additionally, given that '*consumers are not very much aware of a deterioration of quality of a product as long as the price is affordable*'[286], quality degradations in zero-price markets remain largely imperceptible. Similarly, extensive data collection can also spur innovation, example in creating highly efficient digital assistants, thus further complicating this weighing exercise.

The Privacy Paradox

In addition to the general complexities associated with quality as a competitive parameter, there also exist further challenges in analysing privacy as a dimension of quality. Specifically, privacy can only be incorporated in the quality analysis to the extent to which consumers see it as a significant factor of quality (*Microsoft/LinkedIn*); which, ultimately depends on the extent to which consumers value their privacy. This is often very tricky to ascertain due to the Privacy Paradox, i.e., the discrepancy between how much users claim to value their privacy and the extent to which they act upon this preference. In other words - although users say they value privacy, in practice they often do little to protect it.[287]

[285]Manne & Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust' (2015) CPI Antitrust Chronicle (2015) 3.

[286]OECD Quality Report (n 160) 86.

[287]Barth and Jong, 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review' (2017) 34(7) Telematics and Informatics 1038.

For instance, numerous surveys show that online privacy is a genuine concern for consumers.[288] In 2019, 79% Americans were concerned about the way their data was used by companies and 81% believed the potential risks associated with data collection outweighed the benefits.[289] Similarly in Europe, 89% of the population believed that browser default settings should stop their information from being shared, 64% considered that it's not acceptable to monitor online activities in exchange for unrestricted access to a website, while 71% were against user data-sharing without permission, even if it enabled a new service.[290] However, in practice consumers seldom act in a way which reflects such strong preferences for enhanced privacy. Some key reasons for this Privacy Paradox are as follows.[291]

First, user attitudes to privacy are highly '*subjective and idiosyncratic*'[292], and consequently even in the same circumstances different users have significantly different willingness to disclose information.

Second, even for a single individual, user privacy behavior is highly context-specific; and decisions regarding whether to share or withhold personal information and the types of

[288]Winegar and Sunstein (n 193) 428.

[289]Auxier et al., 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' (*Pew Research Center*, 15 November 2019) <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concernedconfused-and-feeling-lack-of-control-over-their-personal-information/> accessed 30 May 2021.

[290]'ePrivacy: consultations show confidentiality of communications and the challenge of new technologies are key questions' (*Commission*, 19 December 2016) < https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are> accessed 31 May 2021.

[291]Kerber (n 185) 859.

[292]Acquisti, Taylor and Wagman (n 164) 446.

information disclosed, depend on the context in which the information is requested and who is requesting it.[293]

Third, the data economy is characterized by a considerable lack of transparency and information asymmetry between platform and users, example due to opaque privacy policies, unauthorized third-party tracking, data fusion etc. Given the importance of information flows to competitive markets[294], such asymmetric information can hamper users' ability to perform a privacy calculus, i.e., to rationally trade-off the costs and benefits of using a platform. It also constrains any predictions about the long-term costs of disclosed and collected data, thereby making it very difficult for users to act on and protect their privacy preferences.[295] This translates into most consumers' attitude being one of '*tick-click-and-hope-for-the-best*'.[296] Additionally, if consumers don't understand how data collection works, they can't make decisions with privacy in mind or discipline businesses over their collection and use of data. Therefore, asymmetric information can also result in an 'adverse selection' or 'lemons' problem; i.e., a situation where higher quality (ex., more privacy protective) goods are driven out of the market.[297]

[293]ibid.

[294]Nitsche and Hinten-Reed, 'Competitive Impacts of Information Exchange' (*Charles River Associates*, 2004) < https://www.e-ca.com/wp-content/uploads/note_on_information_exchange_en.pdf> accessed 31 May 2021.

[295]Kerber (n 185) 859.

[296]Economides and Lianos (n 74) 39. *See also* Stigler Report (n 25) 218.

[297]Akerlof, 'The Market for Lemons: Quality Uncertainty and the Market Mechanism' (1970) 84(3) The Quarterly Journal of Economics 488.

Fourth, privacy-related decisions are also affected by consumer's bounded rationality, cognitive biases and heuristics, and other behavioral decision-making biases.[298] Due to these, consumers often lack the ability to meaningfully understand and engage with privacy policies; and therefore, end up oversharing data or agreeing to lower levels of privacy.[299] For instance, as consumers are often myopic, have self-control problems and are subject to time-inconsistent preferences; they might value the more immediate gratification of divulging their data, to uncertain risks at a future unknown date.[300] Additionally, the status quo bias implies that consumers tend to stick with default privacy settings, which often leads to extensive data sharing.[301] Similarly, due to the 'free effect', consumers may over-appreciate the benefits of the free product while underappreciating privacy in zero-price markets.[302]

Another reason for users not acting on their privacy preferences is the lack of competition and viable alternatives. As users can't bypass dominant platforms and their non-negotiable privacy terms, they are essentially confronted with a take-it-or-leave-it lockup situation with no choice but to accept the sub-optimal privacy policies.[303] The BkM noted how Facebook's power to impose contractual data processing conditions that users did not want

[298]Acquisti, 'Privacy in Electronic Commerce and the Economics of Immediate Gratification' (2004) Proceedings of the 5th ACM Conference on Electronic Commerce 21, 23.

[299]Hoofnagle and Whittington (n 186) 640.

[300]Acquisti, Taylor and Wagman (n 164) 478.

[301]Costa-Cabral and Lynskey (n 67) 24.

[302]Shampanier, Mazar and Ariely, 'Zero as a special price: The true value of free products' (2007) 26 Marketing Science 742.

[303]Pasquale, 'Privacy, Antitrust, and Power' (2013) 20 George Mason Law Review 1009, 1022; Robertson (n 34) 181.

and would not have agreed to, was only possible due to the unavoidability of Facebook as a trading partner.[304]

Along with the general subjectivity surrounding quality as a competitive parameter, these factors also make it difficult to ascertain when privacy is a dimension of quality to consumers and in quantifying the value of such privacy. However, as discussed below, these challenges can be effectively addressed by antitrust authorities (Part 6.4); especially if frameworks like the GDPR are used as internal workable benchmarks for privacy-quality (Part 6.5).

6.4. ADDRESSING KEY CHALLENGES

As discussed above, a key challenge to this ToH is the complexity and imprecision involved in assessing quality, particularly privacy-quality where users' preferences are highly heterogenous and context-specific. Consequently, it could be tricky to ascertain if privacy does comprise a dimension of quality in the first place. However, subjectivity doesn't mean immeasurability, and there exist various mechanisms which may be utilized to measure consumer preferences regarding privacy-quality in antitrust assessments.

An important tool for assessing quality considerations in specific markets is analysing customers' and competitors' views through market investigations, questionnaires, in-house analysis/surveys etc. Notably, such tools have previously been used by the Commission in various cases. Example in *Ryanair/Aer Lingus*[305], where the competition analysis was

[304]Witt (n 120) 42.
[305]*Ryanair/Aer Lingus* (Case COMP/M 4439) Commission Decision C(2007) 3104 [2007] OJ C 10/6 497.

significantly informed by quality parameters, the EC made extensive use of consumer surveys at Dublin airport. Similarly, in *Microsoft/LinkedIn* the Commission undertook a survey of social network businesses to understand whether privacy is an important driver of competition and consumer choice in the market. Admittedly these examples pertain to ex-ante merger assessments, and using similar questionnaires in determining ex-post abuses may be more complex. However, surveys are flexible instruments and can easily be tailored to different circumstances, including for ex-post assessments under Article 102 TFEU.[306] For instance in *Intel* - an Article 102 TFEU case - the EC made use of '*OEM submissions and contemporaneous documents*' while analysing relevant quality considerations, given that they were '*best-placed to come to the soundest judgment as regards their supply needs*'.[307]

As such, competition agencies do have prior experience with subjective and idiosyncratic quality-related consumer preferences; and, a similar use of surveys can also be made while assessing degradations of privacy-quality. Importantly, the increasing number of studies on the Privacy Paradox and behavioral economics can also be used to inform such questionnaires, to make them even better-suited to the data economy.[308]

Other techniques which can also be used to ascertain the relevance of privacy in a given market include actual consumer responses to privacy changes; platforms' evolution of privacy policies in light of different levels of competition; documentary evidence pertaining to platforms' internal decisions/proceedings regarding privacy (ex., the senior management clash between Facebook and Whatsapp over privacy post-merger is indicative of the

[306]OECD Data-Rights Report (n 31) 36.

[307]*Intel* (COMP/37.990) [2009] European Commission Decision D(2009) 3726 final, paras 1698-1699.

[308]Pepper and Gilbert (n 70) 135.

significance of privacy in the market[309]); independent consumer behavioural studies about users' privacy expectations[310] etc.

Interestingly it has also been argued that even if only a few consumers actually act on their privacy preferences, this could still be enough to raise competitive concerns.[311] This is because different consumers care about different things, and marginal consumers (who keep market power in check) might be particularly affected by data protection; and, may even constitute a separate market.[312]

Consequently, competition law has the relevant tools to ascertain consumer views on privacy in a specific market and whether it should form part of product quality. However, the main purpose behind such questionnaires is to explore privacy as a relevant component of the quality dimension in the first place - they may not provide the exact magnitude of *how much* consumers value privacy-quality in light of other relevant parameters, and the exact point at which a privacy degradation should be considered exploitative. In traditional markets this issue is often resolved by relying on prices, and whether the overall price/quality ratio has improved or worsened.[313] However, as this is not feasible in the zero-price data economy, there is a need for an additional threshold (instead of price) against which privacy degradation

[309]Grind and Seetharaman, 'Behind the Messy, Expensive Split Between Facebook and WhatsApp's Founders' (*WSJ*, 5 June 2018) < https://www.wsj.com/articles/behind-the-messy-expensive-split-between-facebook-and-whatsapps-founders-1528208641> accessed 31 May 2021.

[310] BEUC, *Market Definition in EU Competition Law Enforcement: Need for an update* (BEUC's response to the public consultation, 2020) 3 <https://www.beuc.eu/publications/beuc-x-2020-092_beuc_response_public_consultation_on_market_definition.pdf> accessed 31 May 2021.

[311]Costa-Cabral and Lynskey (n 67) 14.

[312]ibid.

[313]Ezrachi and Stucke, 'The Curious Case' (n 160) 228.

warranting antitrust intervention can be analyzed. Incorporating such a threshold also creates an important limiting principle to ensure that intervention is only pursued when necessary. This is further discussed in Part 6.5.

In addition to subjective consumer preferences, asymmetric information and behavioral biases can also distort consumer interest in privacy. Notably, these demand-side market failures can be resolved through data and consumer protection legislations, market investigations, platform-specific regulation and using behavioural economic insights.[314] Similarly, take-it-or-leave-it clauses and a lack of alternatives can also be addressed through a generally competitive market which caters to users' privacy preferences; in which context, merger enforcement and ex-ante regulation can play a critical role. This wider regulatory toolbox and its complementary role in enabling consumers engage meaningfully with privacy as an element of a service's quality, is further detailed in Section 7.

Therefore, there exist various tools which can be used to assess if privacy constitutes an important dimension of quality under competition law. The next step is to identify a clear benchmark for the exact point at which privacy-quality degradation becomes exploitative, i.e., a precise threshold for Article 102 TFEU intervention.

6.5. DATA PROTECTION LAW AS AN ADDITIONAL BENCHMARK

Given the ambiguity in quantifying privacy-quality in the absence of prices, there is a need to provide competition law with relevant normative tools to assess how privacy conditions reflect the quality of a product/service, and a concrete benchmark for Article 102 TFEU intervention.

[314]Stigler Report (n 25) 95-96.

In this context, data protection law – a framework specifically designed to identify and achieve an optimal level of privacy and data collection – can provide such guidance. This includes legislations and guidelines like the GDPR, e-Privacy regulations, the OECD's Privacy Guidelines etc.

Here, an infringement of data protection law or failure to honor rights granted therein, would constitute a clear indication of degraded privacy-quality. Costa-Cabral and Lynskey have extensively opined on how, in the absence of price signals, data protection laws can help assess whether exploitative abuses have occurred; particularly, by looking at whether such laws have been violated, or whether a dominant firm has abused its position to obtain a '*legal decrease in control over personal data or an increase in the extent of processing*'.[315]

Although this may seem similar to the 'External Benchmarks' approach discussed in Section 5 (Part 5.3), there is a key difference in the specific role to be played by privacy laws under this ToH. In viewing privacy as a dimension of quality, i.e., a widely recognized non-price competitive parameter; this approach places data protection law squarely within the internal logic of competition law and also provides a direct connection between privacy and consumer welfare. Here, privacy-quality is assessed like any other attribute of product quality within the antitrust sphere; but in determining exploitative quality degradation, normative guidance is sought from data protection law (instead of price). As such, this approach adopts a neutral stance towards privacy (which is just another aspect of product quality) and avoids the objection that antitrust is being 'instrumentalized' to achieve non-competition aims.[316]

[315]Costa-Cabral and Lynskey (n 67) 18.

[316]Robertson (n 34) 166; Costa-Cabral and Lynskey (n 67) 14.

Additionally, as this ToH focuses not just on excessive data harvesting but a myriad of other privacy-reducing conducts (Part 6.2), it can protect consumers from a wider range of exploitative behaviour. And relevant GDPR principles which can be engaged here range beyond purpose limitation and data minimization[317], to also include integrity and confidentiality (Article 5(1)(f)), the security of processing (Article 32), storage limitation (Article 5(1)(e)), privacy by design and default (Articles 25(1) and (2)), transparency of terms (Article 5(1)(a)) etc. There also exist various means to analyse a platform's adherence to GDPR principles in context of antitrust assessments including expert opinions, business responses to information requests, questionnaires answered by consumers/competitors/market players and other related disclosures.

Further, given that the GDPR also provides for free user choice and consent regarding data collection, this ToH can also be used in cases where platform usage is made conditional on users accepting take-it-or-leave-it privacy terms. Specifically, as per Article 7(4), '*When assessing whether consent is 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*'. Similarly, Recital 49 also provides that '*[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*'. As such, a predominant and particularly exploitative conduct can be sanctioned under this ToH.

[317]GDPR, Articles 5(1)b and 5(1)c.

Therefore, this ToH accounts for a broad range of some of the most problematic privacy-degrading conducts. Additionally, some observers have also argued that where platforms make wholesale privacy-degrading changes to their initial data processing conditions, which users must accept in order to continue using an online service, then such changes should be sanctionable under Article 102 TFEU even if they are otherwise GDPR-compliant[318]; as they can be considered exploitative in the same way that a sudden and unjustified increase in price has been considered abusive. This was recently also acknowledged by FTC Commissioner Rohit Chopra, who noted that dominant platforms can change their already '*complex and draconian*' terms of service suddenly '*to collect and use data more expansively and more intensely*', a behaviour which is consistent with a unilateral price hike that would be difficult to impose in a competitive market.[319]

As such, this ToH comprises a two-step approach where tools discussed in Part 6.4 can determine if privacy is a relevant parameter of quality in the given market, and data protection legislation can provide the threshold for *when* a degradation of privacy-quality is abusive under Article 102(a) TFEU; thereby addressing the key challenges associated with this privacy-quality standard.[320] This can be illustrated as follows:

Example 1: Dominant Platform 'DP' operates a social media platform 'Footbook' and a messaging service 'Howsapp'. Given DP's dominance and lack of viable alternatives,

[318]Family ties (n 67) 18.

[319]Data and Privacy Hearing, 'Testimony of FTC Commissioner Rohit Chopra' (*House Judiciary Committee - Subcommittee on Antitrust, Commercial, and Administrative Law*, 18 October 2019) 3 < https://www.ftc.gov/system/files/documents/public_statements/1549812/chopra_-_testimony_at_hearing_on_online_platforms_and_market_power_part_3_10-18-19.pdf> accessed 31 May 2021.

[320]Colangelo and Maggiolini, 'Data Protection in Attention Markets: Protecting Privacy through Competition?' (2017) 8(6) Journal of European Competition Law & Practice 363.

several users are locked in to both services. DP decides to make the provision of Howsapp contingent on users agreeing to sharing their data with Footbook, despite such data sharing and processing not being essential for the provision of Howsapp's services. In assessing whether such data harvesting is an exploitative abuse of dominance, surveys, in-house reports etc., can first be used to determine if a sufficient number of Howsapps's users view privacy as an aspect of service quality. Once this is established, the next step is determining if DP's conduct degrades privacy-quality to such a degree that it constitutes an exploitative abuse of dominance, using data protection laws as an internal benchmark. Here, since DP's conduct infringes GDPR Article 7(4) (detailed above), it can be concluded that DP's privacy-quality degradation is exploitative under Article 102 TFEU.

Example 2: DP's social media arm – Footbook, collects user data not just on the platform; but, extensively across all webpages visited by its users and where Footbook plug-ins are installed. Such extensive third-party tracking is not necessary for the provision of social media services, but instead is heavily monetized by Footbook through targeted advertising. And given Footbook's complex and lengthy terms of service, users are largely unaware of such ubiquitous third-party tracking and data collection. Here, to assess if Footbook has infringed Article 102 TFEU: First, the competition authority will have to establish that Footbook users view privacy as part of the service quality (using mechanisms discussed in Part 6.4). Then, to determine if the platform's conduct is an exploitative abuse of dominance, data protections laws will be used. Here, users are largely unaware of Footbook's widespread third-party tracking and data harvesting, which breaches the GDPR's transparency and user consent principles.[321] Therefore, this conduct infringes Article 102 TFEU.

[321]Articles 4(11), 5 and 12-14, GDPR.

Finally, although a comprehensive discussion regarding the same is outside the scope of this thesis, data protection legislations can also be incorporated into the design of competition law behavioural *remedies*.[322] Here, using frameworks like the GDPR, antitrust authorities could impose limits on the amount of data harvested, storage length and collection purposes; mandate specific transparency and data monetization requirements; ensure valid consent by requiring firms to provide effective options or to change data collection defaults (from opt-out to opt-in); impose data portability requirements to reduce consumer lock-in[323] etc. Remedies can also be designed to reflect appropriate technological developments, and it can also be queried if platforms can provide the same level of quality in their services without the various insidious impingements on privacy.

Overall, the privacy-quality degradation ToH is a sound approach to sanctioning exploitative data harvesting by dominant platforms under Article 102 TFEU. And given competition enforcers familiarity with using tools like questionnaires, and the presence of a solid benchmark like the GDPR; it is a feasible approach, with high chances of being practically enforced. Finally, this ToH isn't restricted to just the GDPR, but also includes other regulations (current and future), which could provide relevant benchmarks; for instance, data protection provisions in the DMA. Therefore, this is a principled approach that uses data and privacy related regulation as an inner threshold.

[322]Terra Incognita (n 151) 81-82.

[323]Kerber (n 185) 862.

Finally, as mentioned previously, Article 102 TFEU can also be situated in a broader context, with other legislative frameworks playing a complementary role in tackling exploitative data harvesting. This wider enforcement toolbox is discussed in the next Section.

7. ARTICLE 102 TFEU AS PART OF A WIDER ENFORCEMENT TOOLBOX

As established so far, Article 102 TFEU can be used to sanction dominant platform's exploitative data harvesting conducts, specifically using the privacy-quality ToH explored in Section 6.

However, other tools - both within and outside of competition law – can further complement Article 102 TFEU in this sphere. Specifically, they can address broader market characteristics (ex., insufficient information requirements) and demand-side market failures (ex., invalid consent), thereby narrowing the gaps in ex-post antitrust enforcement.

This Section focuses on this wider enforcement toolbox. Part 7.1 highlights the key limitations of Article 102 TFEU in the data economy; and, Part 7.2 discusses the role to be played by other areas of antitrust (merger control and market investigations). The subsequent Parts look at regimes outside competition law. Specifically, Part 7.3 looks at data protection and consumer laws, and Part 7.4 discusses the complementary role to be played by sectoral regulation. Thereafter, Part 7.5 explores the relevance of institutional cooperation in addressing data-related issues arising in the platform economy. Finally, this Section ends with some 'Reflections' on Article 102 TFEU enforcement in light of such complementary regimes, and the need for a balanced approach that does not chill competition and innovation but also ensures competitiveness of markets and consumer welfare (Part 7.6).

7.1. KEY LIMITATIONS OF ARTICLE 102 TFEU

Although Article 102 is a highly effective instrument, it has some limitations when applied in the data economy.

One key limitation is in respect of *timing*. Ex-post competition enforcement is a lengthy procedure and can take years to resolve, with additional time required for the appeal stages; particularly, in complex markets like the data economy. As digital markets are susceptible to a winner-takes-all dynamic, lengthy procedures can be especially harmful and there is '*a risk that, by the time appeal routes are exhausted, the harm will have become entrenched or the market will have "tipped", rendering the competition authority's decision, even if upheld, ineffective'*.[324] For instance, during the seven-year long investigation in the *Google Shopping* case[325], Google continued its self-preferencing behavior which damaged competition irreversibly and also undermined the final remedies. Remarkably, noteworthy developments can still be expected in this case (which is under appeal before the General Court) given the recent CJEU decision in *Slovak Telekom*[326].

To address these timing concerns there has been increasing support for the use of interim measures in antitrust proceedings[327], and to reform the existing framework such that

[324]Letter from Lord Tyrie (CMA Chairman) to Greg Clark MP (Secretary of State for BEIS) (21 February 2019) footnote 16 < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781151/Letter_from_Andrew_Tyrie_to_the_Secretary_of_State_BEIS.pdf> accessed 31 May 2021.

[325]*Google Search (Shopping)* (CASE AT.39740) [2017] C(2017) 4444 final.

[326]Case C-165/19, *Slovak Telekom v European Commission* [2021] Court Reports - general.

[327] 'Statement by Commissioner Vestager on Commission decision to impose interim measures on Broadcom in TV and modem chipset markets' (*Commission*, 16 October 2019) < https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_6115> accessed 31 May 2021; House of Lords, *Online Platforms and the Digital Single Market* (10th Report of Session 2015–16, HL Paper 129, 20

it is better-suited to the digital age.[328] This can be done by addressing underlying procedural and administrative difficulties (ex., restricting the access-to-file process)[329], revising the high standard of proof (ex., in Germany)[330] etc. Enabling more frequent use of interim measures can be particularly beneficial in cases involving exploitative data collection; as otherwise, by the time final remedies are imposed, the platform would have already amassed extensive amounts of data and irreversibly harmed user privacy, with ineffective and difficult-to-implement final remedies. Additionally, even a general use of interim measures in the digital markets sphere, including in exclusionary conduct cases, could be useful in preserving the market structure and limiting the extent to which the market tips.

Notably, timing concerns surrounding Article 102 TFEU enforcement can also be addressed by reforming the standard of appeal in antitrust cases, to one closely resembling a judicial review standard.[331] This could also encourage enforcement by antitrust authorities, as there would be lower risk of being overturned on appeal.

Another significant limitation of Article 102 TFEU in data economies is the type and effectiveness of potential *remedies*. The traditional antitrust remedy of a fine in conjunction

April 2016) 53; Furman Report (n 19) 104; 'The Autorité de la concurrence has ordered interim measures against Google' (*Autorité de la concurrence* 31 January 2019) <https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/31-january-2019-online-advertising-directory-enquiry-services-0> accessed 31 May 2021.

[328]Feases 'Sharpening the European Commission's tools: interim measures' (2020) 16(2-3) European Competition Journal 404.

[329]Furman Report (n 19) 105.

[330]'Amendment of the German Act against Restraints of Competition' (*Bundeskartellamt*, 19 January 2021) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html> accessed 31 May 2021.

[331]Furman Report (n 19) 105

with an order to cease the conduct has limited ability to correct the market, and cannot '*turn the clock back*' or address long-lasting effects of the misconduct.[332] Structural remedies are also considered to be unsuitable for digital markets, as they can often have substantial negative effects for innovation and long-run consumer welfare.[333] Given their flexibility, behavioural remedies are a popular choice in context of novel abuses in the fast-moving data economy.[334] However, such remedies can't correct market characteristics as a whole, and also have some enforcement challenges (example, in monitoring compliance).

These limitations merit a closer consideration of complements to ex-post Article 102 TFEU enforcement. The next Part explores other competition law tools which can be especially helpful in this context.

7.2. OTHER COMPETITION LAW TOOLS

Within the realm of competition law there exist two particularly significant tools which can complement Article 102 TFEU in sanctioning exploitative data harvesting - merger control and market investigations.

Merger control

Historically, there has been little scrutiny of acquisitions by major digital platforms of smaller companies and startups; for instance, between 2008 and 2018 the five largest digital firms

[332]Terra Incognita (n 151) 69.

[333]OECD Quality Zero-price (n 256) 23.

[334]Terra Incognita (n 151) 73.

have collectively made over 400 acquisitions globally, with most of them cleared as is and none prohibited.[335] Given the winner-takes-all dynamic of the platform economy, such underenforcement can condemn the entire industry to a monopoly – an '*irreversible'* change, especially when combined with political power.[336]

Notably, novel elements like privacy, data aggregation, and enhanced data analytical/processing capabilities, have not been easily addressed, or have been ignored as relevant considerations in merger assessments. Consequently, several approved acquisitions have created platforms with highly concentrated data harvesting/combination capabilities and an adverse impact on privacy.[337] Let us briefly review some of the challenges to traditional merger enforcement in the digital realm:

First, there exist various difficulties in predicting the impact of a merger in fast-moving innovative landscapes and on potential competition; and in balancing any potentially detrimental implications (especially when these pertain to user privacy) against important efficiencies in such an uncertain landscape.

Additionally, the reliance on turnover thresholds for notifying mergers and takeovers is also problematic as many digital market transactions entail acquisitions by dominant platforms of much smaller players (with low revenues), and don't meet this benchmark. Notably, some jurisdictions are already contemplating steps to rectify this gap in current enforcement; for instance, by incorporating transaction values in the notification threshold (Germany and Austria) and requiring mandatory notifications for digital sector mergers

[335]Furman Report (n 19) 12.

[336]Stigler report (n 25) 16.

[337]Examples include *Microsoft/LinkedIn, Facebook/Whatsapp* and *Google/DoubleClick.*

(EU[338], UK[339] and Germany[340]). Additionally, the EC also recently published a new Article 22 referral guidance which would allow NCAs to refer transactions falling below the relevant national notification threshold to the Commission.[341]

Further, a large number of transactions in the digital markets sphere are conglomerate mergers. Given that traditional merger enforcement has primarily focused on horizontal transactions, the ToH required in such a conglomerate context are highly underdeveloped. This is further exacerbated by the zero-price nature and multi-sidedness of the data economy, where even the most sophisticated antitrust tools need fine-tuning. Consequently, transactions like *Facebook/Instagram* or *Facebook/Whatsapp*, which have ultimately proven to be harmful, were cleared by enforcers with inadequate scrutiny.[342] As such, there is a definite need to adapt traditional ToH and/or devise new ones; for instance, by focusing on the long-run effects of transactions, considering questions of potential competition, scrutinizing non-price competitive parameters, identifying key drivers for transactions (ex., more consumer data); shifting the burden of proof to the dominant platform, adopting a 'balance of harms' approach to account for the scale and likelihood of harm in merger cases etc.[343] These reforms

[338]Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act) [2020] COM/2020/842 final, Article 12 < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en> accessed 31 May 2021.

[339]CMA, *The CMA's Digital Markets Strategy: February 2021 refresh* (9 Feb 2021) <https://www.gov.uk/government/publications/competition-and-markets-authoritys-digital-markets-strategy/the-cmas-digital-markets-strategy-february-2021-refresh> accessed 31 May 2021.

[340]BkM 'Amendment' (n 330).

[341]Commission Guidance on the application of the referral mechanism set out in Article 22 of the Merger Regulation to certain categories of cases C (2021) 1959 final.

[342]OECD, *Start-ups, Killer Acquisitions and Merger Control – Background Note* (DAF/COMP(2020)5) 20 <https://one.oecd.org/document/DAF/COMP(2020)5/en/pdf> accessed 31 May 2021.

[343]Stigler Report (n 25) 17; Furman Report (n 19) 99; Cremer Report (n 16) 110.

have already been implemented in some jurisdictions. Example, the UK has recently updated its Merger Assessment Guidelines to incorporate parameters like potential competition, non-price related effects etc.; and has also used a non-traditional ToH (loss of potential competition) in its recent Facebook/Giphy investigation.[344] Similarly, the US is also making undoing bad mergers a cornerstone of its antitrust cases against Facebook and Google.[345]

Provided appropriate reforms are introduced, the merger control framework can play a significant complementary role alongside Article 102 TFEU in targeting exploitative data harvesting. This can be direct, where authorities start considering privacy issues in merger assessments thus leading to enhanced privacy protection for users, safeguards against data amalgamation, incentives to compete on privacy etc. It can also be indirect, i.e., efficient merger control providing for a healthy market structure and restricting the number of touchpoints from which data-opolies can harvest data. Example, if Facebook's acquisition of Instagram or Whatsapp had been curtailed/blocked on the grounds of harming potential competition, not only would the market structure remain preserved, but it would have also had a positive impact on user privacy.

However, merger control is only relevant where there is a transaction to be scrutinized. In this context it would be useful to discuss market investigations; i.e., another ex-ante antitrust tool, with general application, which can play a significant complementary role to Article 102 TFEU.

[344]'Facebook's purchase of Giphy raises competition concerns' (*CMA*, 25 March 2021) <https://www.gov.uk/government/news/facebook-s-purchase-of-giphy-raises-competition-concerns> accessed 31 May 2021.

[345]Caffarra and Morton, 'The European Commission Digital Markets Act: A translation' (*VOXEU*, 5 January 2021) < https://voxeu.org/article/european-commission-digital-markets-act-translation.> accessed 31 May 2021.

Market investigations

Market investigations can be highly valuable in addressing antitrust concerns in the digital economy; particularly, as their very function is to identify and remedy markets which have become 'stuck' in bad equilibria and to proactively promote competition.[346] Therefore, this tool can go beyond what ex-post antitrust provisions can achieve, and unlike mergers isn't restricted to a specific transaction.

Market investigations are well placed to account for the wider context, particularly the interplay between competition and other policy areas like privacy, consumer protection etc.; and a variety of interwoven structural and behavioural factors causing competition concerns. This is especially useful for digital markets, where issues frequently arise from a combination of factors like firm conduct, consumer behaviour, economic characteristics etc. Market investigations also provide for flexible remedies, which can be designed to address broad market characteristics like economies of scale and scope, network effects, regulatory and structural barriers and consumer behaviour.

Several jurisdictions have started invoking their market investigation powers in the digital economy. For instance, UK recently investigated the digital market advertising sector, where the CMA found that key platforms (particularly, Google and Facebook) have developed '*such unassailable market positions that rivals can no longer compete on equal terms*'.[347] Similar

[346]Fletcher, 'Market Investigations for Digital Platforms: Panacea or Complement?' (2021) 12(1) Journal of European Competition Law & Practice 44.

[347]CMA 'Digital Advertising Report' (n 50) 5.

investigations have been conducted in Australia[348] and Japan.[349] Also noteworthy is the EC proposal for a New Competition Tool, which will see the EU having an instrument similar to the UK to address competition problems. Specifically, this tool will allow the Commission to open market investigations for designating gatekeepers, investigating systematic non-compliance, examining new services/practices etc.[350]

Therefore, market investigations are a powerful antitrust tool which can be used to support competitive markets and intervene in a pre-emptive manner, especially when seen in conjunction with sector-specific regulations (Part 7.4).

7.3. DATA PROTECTION AND CONSUMER ENFORCEMENT

In addition to tools within the competition law framework, there also exist various external instruments which can complement Article 102 TFEU in addressing extensive data harvesting and privacy degradation by dominant platforms; specifically, data protection and consumer enforcement.

Data protection

Of significance is data protection law - a regime specifically tailored to ensure optimal privacy and data collection levels for users. There exist various frameworks which could be

[348]ACCC, *Digital Platforms* < https://www.accc.gov.au/focus-areas/digital-platforms> accessed 31 May 2021.

[349]'Interim Report Regarding Digital Advertising' (*JFTC*, 28 April 2020) <https://www.jftc.go.jp/en/pressreleases/yearly-2020/April/200428.html> accessed 31 May 2021; 'Report regarding trade practices on digital platforms (Business-to-Business transactions on online retail platform and app store)' (*JFTC*, 31 October 2019) <https://www.jftc.go.jp/en/pressreleases/yearly-2019/October/191031.html> accessed 31 May 2021.

[350] DMA, Articles 14-17.

instrumental in safeguarding user privacy like the GDPR, e-Privacy regulation[351] and OECD Privacy Guidelines.[352] In illustrating how the data protection sphere can complement Article 102 TFEU, this Part focuses specifically on the GDPR.

Key GDPR principles like purpose limitation and data minimization[353] - which provide that data collection must be limited to what is necessary for achieving a specified and legitimate purpose - could limit the volume of data harvested through third-party tracking.[354] And as per some initial observations, since the GDPR came into force third-party cookies on news sites in Europe have declined by 22%.[355] Similarly, principles pertaining to user consent[356] and other rights of data subjects (subject access rights[357], right to be forgotten[358], right to restriction of processing[359], data portability[360] etc.) can be used to limit unauthorized tracking and enhance users' control over their own data. Other relevant principles include

[351]Example, Article 6 (limiting data processing to a specific and necessary purpose and duration); Article 8 (protection of user information); Article 9 (consent requirements for processing user data); Article 10 (information and options in respect of privacy settings).

[352]OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013): Article 7 (collection limitation); Article 9 (purpose specification); Article 8 (data quality principle).

[353]Articles 5(1)b and Article 5(1)c.

[354]Ezrachi and Roberston (n 2) 12.

[355]Libert, Graves and Nielsen, 'Changes in Third-Party Content on European News Websites after GDPR' (*Reuters Institute and Oxford University factsheet*, August 2018) 1 < https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf> accessed 31 May 2021.

[356]GDPR, Articles 6 and 7.

[357]GDPR, Article 15.

[358]GDPR, Article 17.

[359]GDPR, Article 18.

[360]GDPR, Article 20.

specific restrictions on profiling[361]; ensuring transparency[362] (ex., by providing for clear, precise and understandable privacy policies); data security measures[363] (ex., to prevent unauthorized access, accidental loss, destruction of data); privacy by default and design measures[364] (ex., through PETs, pseudonymization and anonymization) etc.

Additionally, certain GDPR principles like data portability (Article 20) can also improve the general market structure, spur competition and enable consumer switching by weakening user lock-in.[365] Similarly, greater interoperability can eliminate the network externalities that drive the winner-takes-all nature of the social media market by allowing technically different systems to communicate with each other. Notably, data portability and interoperability can also be used as antitrust remedies to facilitate market entry, and dissuade dominant platforms from extracting excessive amounts of data from users.

However, there are a few problematic areas in the GDPR; reforming which could enhance the effectiveness of the regime and the complementary role it plays alongside Article 102 TFEU:

First, there have been some concerns that the GDPR is enabling large digital companies to reinforce their own dominance, example Google can now collect more data than the pre-GDPR era; whilst imposing unduly strict compliance duties on smaller firms.[366]

[361]GDPR, Article 22.

[362]GDPR, Article 5(1).

[363]GDPR, Article 32.

[364]GDPR, Article 25.

[365]Kerber (n 185) 862.

[366]Furman Report (n 19) 124, 125.

Consequently, a need to undertake a retrospective assessment of the GDPR's impacts, including on market structure and competition, has been identified.[367]

Second, the GDPR framework is riddled with enforcement and administrative bottlenecks. For instance, using access rights to determine what firms process '*is bewildering and time-intensive'*, with the platform using '*countless attempts to defuse your request*', and ultimately providing an unsatisfactory response or a legally questionable refusal.[368] There also exist multiple obstacles at the regulatory/institutional level, which have severely hampered the effectiveness of the GDPR and redress available to users.[369] Additionally even when detected, appropriate action is often not taken against platforms' privacy-degrading conducts. Example, although the UK's privacy regulator - the Information Commissioner's Office (ICO) - found the AdTech industry to be collecting and sharing people's browsing history in breach of the GDPR; it decided to close the investigation instead of taking any substantive action.[370]

Third, there has been a growing consensus that the current notice-and-consent framework in the GDPR is inadequate to safeguard user privacy. Given that the effectiveness of such consent-based models is determined by users' perception and activism; in practice, they are often undermined by demand-side factors like asymmetric information, consumer

[367]ibid.

[368]Veale, 'Ignore Mark Zuckerberg' (*Slate*, 12 April 2018) <https://slate.com/technology/2018/04/mark-zuckerbergs-misleading-promise-that-eu-privacy-rules-will-apply-to-american-facebook-users.html> accessed 31 May 2021.

[369]Letter from BEUC to the Commissioner for Justice (EC) on GDPR second anniversary – Recommendations for efficient enforcement (25 May 2020) <https://www.beuc.eu/publications/beuc-x-2020-040_gdpr_second_anniversary_-_recommendations_for_efficient_enforcement_letter.pdf> accessed 31 May 2021.

[370] 'Privacy organization open rights group taking the privacy regulator ICO to court in a landmark case' (*Open Rights Group*, 5 November 2020) < https://www.openrightsgroup.org/press-releases/privacy-organisation-open-rights-group-taking-the-privacy-regulator-ico-to-court-in-a-landmark-case/ > accessed 30 May 2021.

inertia and behavioural biases. Even the e-Privacy Regulation adopts a user consent-based approach in determining the legitimacy of third-party tracking (Article 8(1))[371], and is therefore susceptible to similar Privacy Paradox concerns. Additionally, such sole focus on transparency further individualises responsibility for ensuring systems are socially aligned; which fails to give users meaningful control, and often results in the 'transparency fallacy'.[372] Consequently, there exists a broader need to account for such information and rationality problems in the existing data protection frameworks, and to make greater use of behavioural economic insights.[373] In some cases it could be beneficial to use privacy-friendly consumertarian default rules i.e., default privacy rules which follow the preference of a majority of consumers based on '*results of well-designed, scientifically rigorous studies'*; to nudge users into making better choices about the protection of their privacy.[374] Similarly, 'sticky' default rules i.e., stringent constraints on waiving the default in favor of a less data protective setting (which, click-through or simple pop-up boxes don't satisfy), can be used in cases where platforms deploy manipulative interfaces.[375] Additionally, behavioral economic insights can be used to identify situations where such defaults will not work, and suitable top-down regulation can then be used to fill these gaps. Certain internet services (like search engines, social networks etc.) can also be mandated to offer more options to their users like

[371]Ezrachi and Robertson (n 2) 12.

[372]Delacroix and Veale (n 58) 3.

[373]Stigler Report (n 25) 95,96.

[374]ibid 109, 234-237, 228.

[375]ibid 19.

charging a subscription fee in return for minimal data collection.[376] PETs could also play a significant role in this context, example Tide Foundation and its encryption of consumers' personal information such that users can only be targeted with advertisements if they consent and are paid.

Thus, in addition to providing relevant benchmarks for competition law (Sections 5 and 6); the data protection framework can directly target firms' harmful data practices, especially if the abovementioned reforms are introduced, thereby playing a significant complementary role alongside Article 102 TFEU.

Consumer Protection

In addition to data protection, consumer law also has an important complementary role to play alongside Article 102 TFEU in curbing exploitative data harvesting; especially by addressing behavioral biases and asymmetric information flows – significant factors underlying the Privacy Paradox.

Specifically, the lack of transparency in how businesses collect/use data, and how they abuse asymmetric information to mislead or deceive users and extract data without express communication (ex., from a website's tracking cookies), are key consumer protection concerns in the data economy.[377] The consumer enforcement toolbox is well-suited to remedying such issues through instruments like consumer education, nudging, labelling, information disclosure duties, minimum standards for products/services; which can increase

[376]Kerber (n 185) 862.

[377]OECD Quality Zero-price (n 256) 31.

transparency and address key behavioural issues like framing effects, the status quo bias etc. In doing so and rectifying the Privacy Paradox, consumer policy can play a directly complementary role alongside competition enforcement in curbing exploitative data collection.

There exist various significant legislations and guidelines in this context. The OECD recommends that businesses should not deceive or mislead consumers, including in relation to the collection and use of consumers' personal data; and also restricts businesses from using unfair practices and contract terms.[378] At the EU level, protecting privacy as part of users' economic interests, is one of the key objectives of consumer law[379]; and all contract terms and commercial practices relating to the use of personal data have to be in conformity with the UCTD and the UCPD. For instance, the UCTD provides that a standard contract term would be unfair if it '*causes a significant imbalance in the parties' rights and obligations….to the detriment of the consumer*' (Article 3(1)), and also requires written contracts to be drafted in '*plain, intelligible language'* (Article 5). Similarly, as per Article 6(1) of the UCPD, a commercial practice has to '*be regarded as misleading if 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*'. Additionally, the EU P2B Regulation also stipulates a number of requirements for online intermediation services to be more transparent about their practices; like specifying what access business users will have to data provided by them or consumers when using the service (Article 9).

[378]OECD, *Consumer Protection in E-commerce: OECD Recommendation* (2016) 4 <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf> accessed 31 May 2021.

[379]Kerber (n 185) 861; 2014 EDPS Opinion (n 83) 23-26.

These instruments can therefore be useful in curtailing the secret harvesting of data; and, in monitoring and controlling the extent to which service providers can obtain general consent (by way of standardized privacy policies) to niche and unexpected uses of private data.[380] Additionally, using behavioral economics insights could also make such frameworks more robust and better-suited to the platform economy.

Importantly, there has already been some consumer law enforcement in respect of privacy policies of platforms like Google, Facebook, iTunes, Instagram, LinkedIn etc.[381] For instance, Facebook's terms and conditions, and the slogan '*sign up, it's free, and always will be*' have been held to be misleading by the Italian NCA as well as the EU Consumer Protection Cooperation Network for not providing adequate information to consumers on how they were actually paying with their data, which Facebook then monetized.[382] The FTC has also found Facebook guilty of deceiving users about their ability to control the privacy of their personal information, in addition to numerous other consumer actions against business' deceptive privacy and data security practices.[383]

Therefore, consumer law enforcement can address the lack of transparency and asymmetric information in platform economies, and play a crucial complementary role alongside Article 102 TFEU in tackling exploitative data harvesting. Additionally, it can also provide relevant context to antitrust assessments; for instance, in light of the above-mentioned

[380]Monopolkommission, 'Competition policy: The challenge of digital markets' (Special Report No. 68, 1 June 2015) paras 339-341 <https://www.monopolkommission.de/index.php/en/press-releases/52-competition-policy-the-challenge-of-digital-markets> accessed 31 May 2021.

[381]OECD Quality Zero-price (n 256) 31.

[382]OECD, *Good Practice Guide on Consumer Data* (OECD Digital Economy Papers No.290, 2019) 11.

[383]ibid 8.

cases it could be argued that the Düsseldorf Court's assumption (in the German Facebook case) that Facebook's pre-formulated contractual terms were sufficient for an average user to make informed and timely decisions and balance the pros and cons of their conduct, is misplaced. The link between privacy-quality in zero price markets and consumer enforcement has also been explicitly recognized by the OECD:

> *In relation to zero-price products, the application of consumer law is mostly concerned with the provision of information to consumers to enable them to effectively exercise their choice. Its application could be relevant in relation to the privacy and advertising dimensions of quality, in particular to address market failures deriving from information asymmetries and behavioural biases of consumers.*[384]

In addition to consumer and privacy laws, sector-specific regulation is also an important part of the enforcement toolbox.

7.4 PLATFORM SPECIFIC EX-ANTE REGULATION

Given the economics of digital markets and its unique challenges, there is now a growing consensus for implementing specific ex-ante regulation in this sphere and actively promoting competition.[385]

Some jurisdictions have already taken substantial steps in this direction. This includes the EU, which recently outlined proposals with the DMA and the Digital Services Act (DSA); the UK, where a Digital Markets Unit (DMU) is being instituted to oversee the platform economy and to apply a code of conduct to companies with a 'Strategic Market Status'

[384]OECD Quality Zero-Price (n 256) 31.

[385]Stigler Report; Furman Report; Cremer Report; US HJR.

(SMS)[386]; Germany, where competition laws have been amended to play a more regulatory role; Denmark and Australia, which have both recently established digital platform units; Japan, where legislation imposing certain obligations on digital platforms has been implemented etc. Additionally, digital regulatory initiatives are also expected in the US.[387]

Such platform-specific ex-ante regulation has an important complementary role to play alongside Article 102 TFEU in tackling exploitative data harvesting; and as noted in the Cremer Report, there is significant potential for both regimes to positively reinforce each other.[388] To illustrate this, relevant provisions of the DMA and the proposed SMS regime in the UK have been discussed below.

EU – DMA

The DMA is intended to spur competition in the digital market sphere by addressing platforms' anti-competitive practices and high entry barriers. For instance, it subjects 'gatekeepers'[389] to a blacklist (ex., MFN/anti-steering clauses) and grey list (ex., self-preferencing) of specific practices.[390]

In respect of specific data related conducts the DMA has a few key provisions. Article 5(a) which prohibits combining end-user data from different sources without consent, can play an important role in limiting unauthorised third-party tracking (in addition to limiting anti-

[386]CMA Strategy Refresh 2021 (n 339).

[387]White House (n 116).

[388]Cremer Report (n 16) 4, 5.

[389]Article 3.

[390]Articles 5 - 7.

competitive exclusionary conduct). Similarly, Article 13 requires gatekeepers to provide the EC with independently audited descriptions of any consumer profiling techniques, thereby ensuring transparency. Additionally, the DSA's provisions on advertising will also give users immediate information on the sources of ads they see online.[391] Further, the DMA also mandates data interoperability[392], which could help improve the market structure and customer switching.

Notably, there are areas for further improvement in the proposed legislation, especially in respect of protecting consumers and addressing data exploitation by digital gatekeepers; example, by providing end-users with easy-to-use accessible solutions for consent management, strengthening interoperability requirements, restricting data which can be processed/shared for targeted advertising etc.[393] However overall, the draft legislation is a significant step towards improving competition in the digital markets sphere, and plays an important complementary role in addressing exploitative data harvesting by dominant platforms.

UK – the SMS regime

The UK's SMS regime is intended to proactively shape the behaviour of the most powerful tech firms (with 'substantial' and 'entrenched' market power), and will be overseen by the

[391]DSA, Articles 24, 30.

[392]Article 6(1)(f).

[393]EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, 10 February 2021 10, 13; EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, 10 February 2021, 15,16.

DMU within the CMA.[394] This regime includes a new legally binding code of conduct tailored to each firm, and will also enable the DMU to impose specific pro-competition interventions. The code will govern elements of how SMS firms do business with other companies and how they treat their users, and will enforce user-oriented principles of fair trading, open choices, trust and transparency. For instance, platforms will be required to be more transparent about the services they provide and how they are using consumers' data, to give users a choice regarding personalised advertising, not restrict customers from using rival platforms etc.[395]

Therefore, platform-specific regulation can increase competition in digital markets and provide consumers with more control over the collection and use of their data, thus playing a useful complementary role in curtailing dominant firms' exploitative data harvesting. And although there are certain inherent risks in regulation (ex., rigidity, chilling innovation, unintended consequences etc.); the DMA/DSA and the SMS regime appear to have been designed with such drawbacks in mind, and are both highly flexible and participative regimes.

Notably, for optimum effectiveness of this wider enforcement toolbox, there is a definite need for institutional cooperation among the regimes.

[394]CMA Strategy Refresh (n 339).

[395]Venier, 'UK and EU race towards regulating digital markets: who is winning?' (*Inline*, 24 February 2021) <https://www.inlinepolicy.com/blog/uk-and-eu-race-towards-regulating-digital-markets-who-is-winning> accessed 31 May 2021.

7.5 NEED FOR INSTITUTIONAL COOPERATION

For antitrust, consumer and data protection, and ex-ante regulation to efficiently complement each other, it is important to ensure institutional cooperation across the frameworks.

Key areas for coordination include identifying potential consumer harms arising from a data-driven economy, improving consumer choice, updating analytical tools to predict and assess how mergers/other restraints can be harmful, providing guidance to businesses, conducting market studies/investigations, seeking advisory opinions, identifying antitrust remedies, internalizing data/consumer protection concerns in competition assessments etc.[396]

The need for closer dialogue across these spheres has been previously stressed upon by the EDPS.[397] It also recommended establishing a 'Digital Clearinghouse' as a voluntary network of regulators which would be responsible for '*using data protection and consumer protection standards to determine "theories of harm" relevant to merger control cases and to cases of exploitative abuse...*'; facilitating information sharing, proposing regulatory solutions in certain markets, and assessing the impact of remedies.[398] Similarly, the OECD has also recognized the potential for coordinated interventions among these regimes.[399]

[396]Stucke and Grunes (n 11) 325-334.

[397]2014 EDPS Opinion (n 83); EDPS, *Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data* (2016) 15.

[398]2016 EDPS Opinion 15.

[399]OECD Quality Zero-price (n 256) para 140.

Here, the recent establishment of the Digital Regulation Cooperation Forum (DRCF) in the UK is particularly notable.[400] The DRCF comprises of the CMA, ICO, Ofcom and most recently the FCA; and has been established to ensure enhanced cooperation and to deliver effective, efficient and coherent regulation across digital markets for the benefit of industry and consumers. Notably, the CMA and ICO have already published a joint statement signaling their intent to focus on policy synergies and working together in data markets.[401]

There have also been proposals for the development of a common strategy across antitrust, consumer and data protection laws[402]; particularly by using the notion of 'fairness' (which underpins all three policy areas) to '*bridge the gap*' across these bodies of law, and accordingly align substantive protections and enforcement mechanisms.[403]

7.6 REFLECTIONS

Article 102 TFEU can be viewed as part of a wider enforcement toolbox, with significant scope for the various frameworks to complement each other and target exploitative data harvesting.

[400]'Digital Regulation Cooperation Forum: embedding coherence and cooperation in the fabric of digital regulators' (*CMA*, 4 May 2021) <https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-embedding-coherence-and-cooperation-in-the-fabric-of-digital-regulators> accessed 31 May 2021.

[401]CMA and ICO, 'Competition and data protection in digital markets: a joint statement between the CMA and the ICO (19 May 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf> accessed 31 May 2021.

[402]Kerber (n 185) 866.

[403]Graef, 'Bridging the Gap' (n 243).

Specifically, consumer and data protection authorities can address certain demand-side characteristics in the platform economy and set the stage for greater quality competition. Similarly, platform-specific regulation, merger control and market investigations can be used to rectify problematic market characteristics, drive competition in the data economy and provide users with more control over their data. And in cases where despite these frameworks fulfilling their respective mandates dominant platforms still abuse their market power to exploitatively harvest data from users, Article 102 TFEU can be used to rectify such specific ex-post violations of competition law.

Therefore, this wider toolbox can remedy the market as a whole (albeit in different ways and at different points), whilst ex-post Article 102 TFEU enforcement can rectify specific failures (and not systemic market failures). As such, this complementary framework ensures a balanced approach that does not chill competition and innovation, but ensures competitiveness of markets and consumer welfare.

CONCLUSION

Is their hubris so great, their assumed power so unassailable, that they see themselves as completely untouchable?[404]

- Benjamin Garfield, in light of Amazon's data security and privacy lapses

Dominant platforms are increasingly acquiring consumer data in exploitative ways and with significant harmful implications for users, including a degradation of their privacy. Companies are able to impose such exploitative data harvesting terms on users only because of their market power and the lack of alternatives; thereby, warranting antitrust enforcement through Article 102 TFEU. Traditional ToH, which are primarily centered around prices, are inappropriate in this context given the unique characteristics displayed by the zero-price data economy; and this thesis explored the possible use of alternate ToH which can sanction such conduct.

As discussed, there are two potential ToH in this context, and both are theoretically feasible (to varying degrees). However, needless to say, antitrust intervention should not be taken lightly and should include appropriate limiting principles. Accordingly, this thesis examined both ToH in detail but singled out *privacy-quality degradation* as the better, more feasible and practically enforceable approach. It includes the use of tools like surveys/questionnaires etc., which antitrust authorities already have prior experience with; and also weaves the data protection benchmark within the internal logic of competition law, thereby avoiding the objection that antitrust is being instrumentalized to achieve the goals of

[404]Manancourt (n 167).

data protection law. Under this approach, the exploitative harvesting of data falls squarely within the remit of Article 102 TFEU – both from a theoretical and practical enforcement perspective – without otherwise widening the boundaries of EU competition law. Therefore, *privacy-quality degradation* forms a viable ToH which can and should be used to address instances in which the market fails to deliver.

Additionally, the aim of this thesis is not to argue for unlimited inclusivity – in fact, it recognizes the various nuances involved and emphasizes how competition law is not the panacea for everything. Instead, it offers a balanced approach with ex-post enforcement being complemented by relevant ex-ante tools, including from external legislative frameworks. Specifically merger control, market investigations, data/consumer protection laws and platform-specific regulation have a significant complementary role to play in this context. By engaging this wider toolbox, an optimal functioning of all regulatory frameworks – including Article 102 TFEU – can be ensured; and exploitative data harvesting and privacy-reduction can be tackled efficiently.

In conclusion, exploitative data harvesting by dominant platforms can be sanctioned as an Article 102 TFEU violation using the *privacy-quality degradation* ToH. This is a well-balanced approach which ensures that competition law isn't being unnecessarily broadened; but conducts which can and should be sanctioned through ex-post Article 102 enforcement, are not being ignored merely because of the novelty of the data economy and the traditional price-centricity of antitrust. Given the increasing focus on the gravity of such conducts and the privacy-antitrust intersection, enforcement action by the Commission can also be expected in this sphere.

BIBLIOGRAPHY

ACM extends its investigation into orphan drug CDCA-Leadiant' (*ACM,* 29 June 2020).

Acquisti, 'Privacy in Electronic Commerce and the Economics of Immediate Gratification' (2004) Proceedings of the 5th ACM Conference on Electronic Commerce 21.

Acquisti, Taylor and Wagman, 'The Economics of Privacy' (2016) 54(2) Journal of Economic Literature 442.

Acqusiti and Wagman, 'The Economics of Privacy' (2016) 52(2) Journal of Economic Literature, Sloan Foundation Economics Research Paper No. 2580411.

Akerlof, 'The Market for Lemons: Quality Uncertainty and the Market Mechanism' (1970) 84(3) The Quarterly Journal of Economics 488.

Akman, 'Searching for the Long-Lost Soul of Article 82 EC' (2009) 29(2) Oxford Journal of Legal Studies 267-303.

Alessandra Venier, 'UK and EU race towards regulating digital markets: who is winning?' (*Inline*, 24 February 2021).

Almunia, 'Competition and personal data protection' (Privacy Platform event: Competition and Privacy in Markets of Data, Brussels, 26 November 2012).

'Amendment of the German Act against Restraints of Competition' (*Bundeskartellamt,* 19 January 2021).

'Antitrust: Commission opens formal investigation into Aspen Pharma's pricing practices for cancer medicines (*Commission,* 14 May 2017).

‘Antitrust: Commission accepts commitments by Aspen to reduce prices for six off-patent cancer medicines by 73% addressing excessive pricing concerns’ (*Commission,* 10 February 2021).

Auxier et al. (2019), ‘Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information’ (*Pew Research Center,* 15 November 2019).

Bania, ‘The role of consumer data in the enforcement of EU competition law’ (2018) 14(1) European Competition Journal 38.

Barth and Jong, ‘The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review’ (2017) 34(7) Telematics and Informatics 1038.

BEUC, *Market Definition in EU Competition Law Enforcement: Need for an update* (BEUC’s response to the public consultation, 2020).

Binns and Bietti, ‘Dissolving Privacy, One Merger at a Time: Competition, Data and Third-Party Tracking’ (2020) 36 Computer Law & Security Review 6.

Binns et al., ‘Measuring third party tracker power across web and mobile’ (2018) arXiv:1802.02507 3.

Binns et al., ‘Third party tracking in the mobile ecosystem’ (2018) ACM WebSci’18.

Biddle, ‘In Court, Facebook Blames Users For Destroying Their Own Right To Privacy’ (*The Intercept,* 14 June 2019).

Greif, ‘Study: Google Is the Biggest Beneficiary of the GDPR’ (*Cliqz,* 10 October 2018).

Bostoen, ‘Online Platforms and Pricing: Adapting Abuse of Dominance Assessments to the Economic Reality of Free Products’ (2019) 35(3) Computer Law & Security Review 263.

Botta and Wiedemann, ‘EU Competition Law Enforcement Vis-À-Vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita’ (2018) Max Planck Institute for Innovation & Competition Research Paper No. 18-08.

Botta and Wiedemann, ‘Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision’ (2019) 10(8) Journal of European Competition Law & Practice 475.

‘Bundeskartellamt prohibits Facebook from combining user data from different sources’ (*Bundeskartellamt*, 7 February 2019).

Buttarelli, ‘Keynote Speech’ (Joint ERAEDPS Seminar on Competition Rebooted: Enforcement and personal data in digital markets, Brussels, 24 September 2015).

Calo, ‘Digital Market Manipulation’ (2014) 82(4) The George Washington Law Review 995.

Caffarra and Morton, ‘The European Commission Digital Markets Act: A translation’ (*VOXEU*, 5 January 2021).

Cisco, *The Internet of Everything* (IoE Value Index Study, 2013).

CMA and ICO, ‘Competition and data protection in digital markets: a joint statement between the CMA and the ICO (19 May 2021).

CMA Policy Paper, ‘The CMA’s Digital Markets Strategy: February 2021 refresh’ (9 Feb 2021).

‘CMA finds drug companies overcharged NHS’ (*CMA*, 15 July 2021).

Colangelo and Maggiolino, ‘Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the US’ (2018) 8(3) International Data Privacy Law 224.

Colangelo and Maggiolini, ‘Data Protection in Attention Markets: Protecting Privacy through Competition?’ (2017) 8(6) Journal of European Competition Law & Practice 363.

‘Commission approves acquisition of LinkedIn by Microsoft, subject to conditions’ (*Commission*, 6 December 2016).

Competition Policy and Consumer Rights on Oversight of the Enforcement of the Antitrust Laws, ‘Statement of Assistant Attorney General Makan Delrahim’ (*U.S. Senate Subcommittee on Antitrust*, 17 September 2019).

Condorelli and Padilla, ‘Harnessing Platform Envelopment in the Digital World’ (2020) 16(2) Journal of Competition Law & Economics 143.

Cook, ‘Keynote Address’ (40th International Conference on Data Protection and Privacy, Brussels, 24 October 2018).

Cooper, ‘Privacy and antitrust: Underpants Gnomes, the First Amendment, and subjectivity’ (2013) 20(4) George Mason Law Review 1129.

Costa-Cabral and Lynskey, ‘Family ties: The intersection between data protection and competition in EU law’ (2017) 54 CML Rev.

Data and Privacy Hearing, ‘Statement by Margrethe Vestager, European Commissioner for Competition’ (*House Judiciary Committee - Subcommittee on Antitrust, Commercial, and Administrative Law*, 6 September 2019).

Data and Privacy Hearing, 'Testimony of FTC Commissioner Rohit Chopra' (*House Judiciary Committee - Subcommittee on Antitrust, Commercial, and Administrative Law*, 18 October 2019).

Data and Privacy Hearing, 'Testimony of Tommaso Valletti, Professor of Economics, Imperial College Business School' (*House Judiciary Committee - Subcommittee on Antitrust, Commercial, and Administrative Law*, 18 October 2019).

Davilla, 'Is big data a different kind of animal? The treatment of big data under the EU competition rules' (2017) 8 JECLAP 370, 381.

Delacroix and Veale, 'Smart Technologies and Our Sense of Self: Going Beyond Epistemic Counter-Profiling' in Hildebrandt, M and O'Hara, K (eds), *Life and the Law in the Era of Data-Driven Agency* (Edward Elgar, 2020).

'Digital Regulation Cooperation Forum: embedding coherence and cooperation in the fabric of digital regulators' (*CMA*, 4 May 2021).

DLA Piper, 'Aspen: Quick Fix But Missed Opportunity' (*Kluwer Competition Law Blog*, 23 October 2020).

Directorate-General for Competition (European Commission), *Competition Policy for the Digital Era* (2019).

Donoghue and Padilla, *Excessive Pricing in The Law and Economics of Article 102 TFEU* (3rd edn, Hart Publishing 2019) 733-799.

Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' (2018) Max Planck Institute for Innovation and Competition Research Paper No. 18–23.

'Dusseldorf Court Asks ECJ To Review Facebook Data Case' (*Competition Policy International*, 24 March 2021).

Dwoskin, 'Apps Track Users—Once Every 3 Minutes' (*WSJ*, 23 March 2015*).*

Economides and Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective' (2021) Journal of Competition Law and Economics 1.

'ePrivacy: consultations show confidentiality of communications and the challenge of new technologies are key questions' (*Commission,* 19 December 2016).

Esayas, 'Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law' (2018) 8(3) International Data Privacy Law 181.

Esayas, 'Privacy-As-A-Quality Parameter: Some Reflections on the Scepticism' (2017) Stockholm University Research Paper No. 43.

Espinoza, 'German groups file Apple antitrust complaint as it makes privacy changes' (*Financial Times,* 26 April 2021).

EU's Vestager Says Google's Planned Removal Of Third-Party Cookies Is An Antitrust Concern' (CPI, 25 April 2021).

Evans and Padilla, 'Excessive Prices: Using Economics to Define Administrable Legal Rules' (2005) 1(1) Journal of Competition Law & Economics 97.

Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (2014).

Ezrachi, ‘The Goals of EU Competition Law and the Digital Economy’ (2018) BEUC Discussion paper.

Ezrachi and Gilo (2008) ‘Are Excessive Prices Really Self-Correcting?’ (2008) 5(2) Journal of Competition Law and Economics 249.

Ezrachi and Robertson, ‘Competition, market power and third-party tracking’ (2019) 42 World Competition 1.

Ezrachi and Stucke, ‘Digitalisation and its impact on innovation’ (2020) European Commission Working Paper, 60.

Ezrachi and Stucke, ‘The Curious Case of Competition and Quality’ (2015) 3(2) Journal of Antitrust Enforcement 227.

Ezrachi and Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016).

‘Facebook’s purchase of Giphy raises competition concerns’ (*CMA*, 25 March 2021).

‘Fact sheet: Executive Order on Promoting Competition in the American Economy’ (*The White House*, 9 July 2021).

Feases ‘Sharpening the European Commission’s tools: interim measures’ (2020) 16(2-3) European Competition Journal 404.

Fletcher, ‘Market Investigations for Digital Platforms: Panacea or Complement?’ (2021) 12(1) Journal of European Competition Law & Practice 44.

FTC, *Hearings on Competition and Consumer Protection in the 21st Century* (October 2020).

FTC Statement Concerning Google/DoubleClick (File No 071-0170, 20 December 2007).

Gal, 'Abuse of Dominance- Exploitative Abuses' in Lianos and Geradin (eds), *Handbook on European Competition Law* (Edward Elgar 2013) 385–422.

Gal and Aviv, 'The Competitive effects of the GDPR' 2020 16(3) Journal of Competition Law & Economics 349, 350.

Gal, 'Monopoly Pricing as an Antitrust Offense in the US and the EC: Two Systems of Belief About Monopoly?' (2004) 49 Antitrust Bulletin.

Gebicka and Heinemann, 'Social Media & Competition Law' (2014) 37(2) World Competition 165.

Gladicheva 'EU privacy rules key to competition analyses, head of France antitrust watchdog says' (*GCR Live: 7th Annual Telecoms, Media & Technology,* 4 May 2018).

'Google's New Privacy Moves Causes US Antitrust Concerns' (*CPI,* 18 March 2021).

Graef, Inge et al, 'Fairness and Enforcement: bridging Competition, Data Protection and Consumer Law' (2018) 8(3) International Data Privacy Law 200.

Graef, 'Speech on Data Silos' (The Florence Competition Summer Conference, Hybrid, 25 June 2021).

Grind and Seetharaman, 'Behind the Messy, Expensive Split Between Facebook and WhatsApp's Founders' *The Wall Street Journal* (5 June 2018).

Haucap, 'Data Protection and Antitrust: New Types of Abuse Cases? An Economist's view in light of the German Facebook Decision' (*CPI Antitrust Chronicle,* February 2019).

Henderson and Askew, ‘Case Preview: Lloyd v Google LLC’ (*UK Supreme Court Blog*, 28 April 2021).

Holmes, ‘Climate change, sustainability, and competition law’ (2020) 8(2) Journal of Antitrust Enforcement 354.

Hoofnagle and Whittington, ‘Free: Accounting for the Costs of the Internet’s Most Popular Price*’* (2014) 61 UCLA Law Review 606.

House of Lords, *Online Platforms and the Digital Single Market* (10th Report of Session 2015–16, HL Paper 129, 20 April 2016).

Interim Report Regarding Digital Advertising’ (*JFTC*, 28 April 2020).

Irakiza, ‘The Charter of Fundamental Rights, the Aims of EU Competition Law and Data Protection: Time to Level the Playing Field’ (2021) Singapore Journal of Legal Studies 39.

‘Italian Competition Authority fines Aspen for excessive anticancer drug price increase’ (*Ashurst*, 11 November 2016).

Kalimo and Mejcher, ‘The concept of fairness: Linking EU competition and data protection law in the digital marketplace’ (2017) 42 EL Review 210.

Kanter, ’Antitrust Nominee in Europe Promises Scrutiny of Big Tech Companies’ (*The New York Times*, 3 October 2014).

Karova and Botta, ‘Sanctioning Excessive Energy Prices as Abuse of Dominance: Are the EU Commission and the National Competition Authorities on the Same Frequency?’ in Parcu, Monti and Botta (eds), *Abuse of Dominance in EU Competition Law: Emerging Trends* (Edward Elgar 2017) 169–84.

Kerber, ‘Digital markets, data, and privacy: Competition law, consumer law and data protection’ (2016) 11 Journal of Intellectual Property Law & Practice 856.

Knapp and Busvine, ‘Top German court reimposes data curbs on Facebook’ (*Reuters*, 23 June 2020).

Kokkori and Lianos, *The reform of EC Competition law: New Challenges* (Kluwer Law International 2009).

Krishnamurthy, Naryshkin and Wills, ‘Privacy Leakage vs. Protection Measures: The Growing Disconnect’ (2011) Proceedings of the Web 2.0 Security and Privacy Workshop 5.

Kuenzler, ‘Direct Consumer Influence—The Missing Strategy to Integrate Data Privacy Preferences into the Market’ (2020) 39 Yearbook of European Law 423.

Kuner et al, ‘When two worlds collide: the interface between competition law and data protection’ (2014) 4(4) International Data Privacy law 247.

Letter from BEUC to the Commissioner for Justice (EC) on GDPR second anniversary – Recommendations for efficient enforcement (25 May 2020).

Letter from Lord Tyrie (CMA Chairman) to Greg Clark MP (Secretary of State for Business, Energy and Industrial Strategy) (21 February 2019).

Libert, Graves and Nielsen, ‘Changes in Third-Party Content on European News Websites after GDPR’ (*Reuters Institute and Oxford University factsheet*, August 2018).

‘Liothyronine tablets: suspected excessive and unfair pricing’ (*CMA,* 25 October 2016).

Lomas, ‘Antitrust case against Facebook’s ‘super profiling’ back on track after German federal court ruling’ (TechCrunch, 23 June 2020).

Lomas, ‘France’s competition authority declines to block Apple’s opt-in consent for iOS app tracking’ (*TechCrunch*, 17 March 2021).

Lowe, ‘How different is EU anti-trust? A route map for advisors’ (Speech at ABA 2003 Fall Meeting, Brussels, 16 October 2003).

Malgieri and Custers, ‘Pricing Privacy – the Right to Know the Value of Your Personal Data’ (2018) 34 Computer Law & Security Review 289.

Manancourt, ‘Millions of people’s data is at risk’ — Amazon insiders sound alarm over security’ (*Politico*, 24 February 2021).

Manne & Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust’ (2015) CPI Antitrust Chronicle (2015).

Manne and Wright, ‘Google and the Limits of Antitrust: The Case Against the Antitrust Case Against Google’ (2011) 34(1) Harvard Journal of Law and Public Policy.

Margarethe Vestager, ‘Making Data Work For Us’ (Data Ethics event on Data as Power, Copenhagen, 9 September 2016).

Mattioli and Lombardo, ‘Amazon Met With Startups About Investing, Then Launched Competing Products’ (*The Wall Street Journal*, 23 July 2020*).*

McDonald and Cranor, 'The Cost Of Reading Privacy Policies' (2008) 4(3) I/S: A Journal of Law and Policy for the Information Society 543.

Melamed and Petit, ‘The Misguided Assault on the Consumer Welfare Standard in the Age of Platform Markets’ (2019) 54 Review of Industrial Organisation 54.

‘Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions’ (*Commission* 17 December 2020).

Monopolkommission, ‘Competition policy: The challenge of digital markets’ (Special Report No. 68, 1 June 2015).

Moorcroft and Le Strat, ‘The rise of big data: The intersection between competition law and customer data’ (2018) 38 Licensing Journal 8.

Newman, ‘Antitrust in zero-price markets: foundations’ (2015) 164 University of Pennsylvania Law Review 149.

Newman, ‘The costs of lost privacy: Consumer harm and rising economic inequality in the age of Google’ (2014) 40 William Mitchell Law Review 849.

Nitsche and Hinten-Reed, ‘Competitive Impacts of Information Exchange’ (*Charles River Associates,* 2004).

Ohlhausen, Online Platforms and Market Power Part 2: Innovation and Entrepreneurship hearing (16 July 2019).

Osborne, ‘Google fails to quash Incognito mode user tracking, privacy lawsuit’ (*ZDNet* , 15 March 2021)**.**

Ozer, ‘The WhatsAppocalypse: Turkish Competition Board Launches In-depth Investigation Against Facebook And WhatsApp’ (*Mondaq* 12 January 2021).

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

Pasquale, ‘Privacy, Antitrust, and Power’ (2013) 20 George Mason Law Review 1009.

Pepper and Gilbert, 'Privacy Considerations in European Merger Control: A Square Peg for a Round Hole' (2015) 5 Antitrust Chronicle Competition Policy International.

'Phenytoin sodium capsules: suspected unfair pricing' (*CMA*, 18 December 2015).

Podszun, 'Digital ecosystems, decision-making, competition and consumers – On the value of autonomy for competition' (2019) SSRN.

'Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive' (*Bundeskartellamt*, 19 December 2017).

'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (EDPS Preliminary Opinion, 2014).

'Privacy organization open rights group taking the privacy regulator ICO to court in a landmark case' (*Open Rights Group*, 5 November 2020).

'Proceeding against Google based on new rules for large digital players (Section 19a GWB) – Bundeskartellamt examines Google's significance for competition across markets and its data processing terms' (*Bundeskartellamt*, 25 May 2021).

Purra and Carlsson, 'Third-Party Tracking on the Web: A Swedish Perspective' (IEEE 41st Conference on Local Computer Networks (LCN), 2016).

'Report regarding trade practices on digital platforms (Business-to-Business transactions on online retail platform and app store)' (*JFTC*, 31 October 2019).

Robertson, 'Antitrust Law and Digital Markets: A Guide to the European Competition Law Experience in the Digital Economy' (2020) REWI.

Robertson, ‘Excessive data collection: Privacy considerations and abuse of dominance in the era of big data’ (2020) 57(1) Common Market Law Review 161.

Sakamaki, ‘Digital platforms' handling of consumer data to be scrutinized under antitrust law in Japan’ (*Mlex* 29 August 2019).

Schelter and Kunegis, ‘Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers’ (2016) Proceedings of the ICWSM 679.

Schneider, ‘Testing Art.102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt’s investigation against Facebook’ (2018) 9(4) Journal of European Competition Law & Practice.

Scott, ‘In battle for privacy, antitrust watchdogs throw their hat in the ring’ (*Politico*, 24 May 2021).

Shampanier, Mazar and Ariely, ‘Zero as a special price: The true value of free products’ (2007) 26 Marketing Science 742.

Singh and Mishra, ‘CCI’s Investigation into WhatsApp Service Policy Update: Mapping the Scope of Regulation of Privacy Policy vis-à-vis Competition Act, 2002’ (*Kluwer Competition Law Blog*,19 April 2021).

Sokol and Comerford, ‘Does antitrust have a role to play in regulating big data?’ in Blair and Sokol (eds), *The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech* (CUP 2017).

Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkley Business Law Journal 39 (2019).

Srinivasan, 'The intersection of privacy, data and competition' (*Promarket*, 26 October 2019).

'Statement by Commissioner Vestager on Commission decision to impose interim measures on Broadcom in TV and modem chipset markets' (*Commission*, 16 October 2019).

'Statement on Commission decision to fine Google euro 2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service' (*European Commission*, 27 June 2017).

Statement by Thomas von Danwitz (*19th International Conference on Competition in Berlin (IKK*), 15 March 2019) reported by Rupprecht Podszun.

Stolton, 'Don't ignore platforms 'combining services' in Digital Markets Act, Netherlands says' (*Euractiv* 17 February 2021).

Stucke & Grunes, *Big Data and Competition Policy* (1st edn, OUP 2016).

Stucke, 'Should we be concerned about Data-opolies?' (2018) 2 Georgetown Law Technology Review 275.

Submission from Ryan (Brave) and Lynskey on Competition issues in digital markets to the CMA (7 October 2019).

Swire, 'Protecting Consumers: Privacy Matters in Antitrust Analysis' (*Center for American Progress*, 19 October 2007).

The Autorité de la concurrence has ordered interim measures against Google' (*Autorité de la concurrence* 31 January 2019).

'The Maritime and Commercial Court: CD Pharma has abused its dominant position by charging an excessive and unfair price for the drug Syntocinon' (*Danish Competition and Consumer Authority,* 3 March 2020).

UK Watchdog To Probe Google Chrome Changes Over Antitrust Concerns' (*CPI,* 10 January 2021).

Veale, 'Ignore Mark Zuckerberg' (*Slate,* 12 April 2018).

Vestager, 'Keynote Speech' (The Florence Competition Summer Conference, Hybrid, 24 June 2021).

Volmar and Helmdach, 'Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation' (2018) 14(2-3) European Competition Journal 195.

Whittaker, 'Researchers find 540 million Facebook user records on exposed servers' (*Techcrunch,* 3 April 2019).

Williams, 'How Facebook Could Use Giphy to Collect Your Data' (*Onezero,* 15 May 2020).

Winegar and Sunstein, 'How Much Is Data Privacy Worth? A Preliminary Investigation' (2019) 42 Journal of Consumer Policy 425.

Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct – The German Facebook Case*'* (2021) 66(2) The Antitrust Bulletin 276,280.

Wyatt, 'Edith Ramirez Is Raising the FTC's Voice' (*The New York Times*, 22 December 2014).