Abate, Serafino

Conference Paper

Antitrust and consumer enforcement in data markets – Are new theories of harm based on privacy degradation hitting the mark?

29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?", Trento, Italy, 1st - 4th August, 2018

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Abate, Serafino (2018) : Antitrust and consumer enforcement in data markets – Are new theories of harm based on privacy degradation hitting the mark?, 29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?", Trento, Italy, 1st - 4th August, 2018, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/184924

Antitrust and consumer enforcement in data markets – Are new theories of harm based on privacy degradation hitting the mark?

Working paper

Serafino Abate[1]

1. Introduction

The part of the economy that depends, directly or indirectly, fully or partially, on the flow and analysis of data is growing of importance[2]. Data-driven businesses are spilling over from the online to the offline economy, changing traditional industries. They are set to become pervasive in the coming decade, with the rise of the industrial internet, the development and adoption of AI, and the advent of new, more advanced networks. As a result, it is not surprising to find that antitrust enforcement in data markets is rising, and the nature of it is in part changing. This raises different issues that are relevant for competition policy in general, antitrust enforcement and consumer protection.

Firstly, alongside traditional theories of harm, new theories of harm are being tested. Some of the recent enforcement cases based on privacy degradation aim at detecting whether or not some platforms have abused their dominance and exploited their customers in the form of data harvesting which goes behind what is permitted ("data exploitation"). Due to the unique nature of data markets and its economics, these new theories of harm rise issues with respect to remedies that are worth considering further.

This working paper focuses on the first aspect, namely to consider whether new exploitative theories of harm based on privacy degradation are plausible. This is very important and poses for me the first order question in the overall assessment of how digital markets works, namely whether the "data for free services" implicit agreement that underpins much of the internet is *structurally* biased towards abuse in the form of data exploitation resulting from privacy degradation. There has been of late a surge of enforcement cases of late in different jurisdiction. Most have been triggered by Facebook's behaviour in respect of its acquisition

[1] Director, Competition Economics, GSMA.

[2] A data economy monitoring initiative for the EU finds that the value of the data economy in the EU could reach 700 Bn Euros by 2020, and its share of the GDP could be as high as 6% in some Member States, see http://datalandscape.eu/european-data-market-monitoring-tool-2018

of WhatsApp and, in relation to its sharing of users data with third party (in particular in relation to the Cambridge Analitica scandal[3], where the users data has been misused to manipulate users/voters). In the case of the WhatsApp acquisition, Facebook's decision to merger the data of its customers with that of the users of WhatsApp has triggered many investigations by national authorities. As this was a specific voluntary undertaking given by Facebook at the time of the merger (i.e. that it would not merger the data of the users of the two platforms), some authorities felt that it infringed not only consumer rights in relation to the treatment of their data (their right to privacy), but that it also potentially constituted an abuse of dominance in the form of privacy degradation (as is the case for the German's *Bundeskartellamt* investigation, and the Italian one by the *Autorita' Garante della Concorrenza e del Mercato,* AGCM).

As a result, in this paper I have decided to focus mainly on the recent enforcement cases against Facebook, as well as analysing the recent approval of Microsoft's acquisition of LinkedIn, where the EC's Directorate General for Competition (DG Comp) puts forward in their assessment a theory of harm based on privacy degradation.

What we are looking for, ideally, are potential impacts that are, *ex post,* observable and measurable, and whether they capture underlying economic effects that are not currently captured by existing theories of harm. These impacts, to be economically meaningful, need to be linked to consumer preferences and economic welfare. There are two aspects to this evaluation. First, there are the consumer preferences. This comprises, as a general level, the personal preferences of the individual, and the general societal preferences, which provides the context for the individual preferences. Second, there is the economic impact on all the economic actors. Of particular significance in this assessment are an evaluation of how value is created and distributed, how the economic power and relative bargaining power of the actors plays out, including how consumer could potentially retaliate if privacy is degraded, which can tell us how effective the potential abusive behaviour is likely to be.

This paper first considers what is the right economic framework to analyse the new theories of harm and how they link to existing theories of harm. We then review the recent enforcement cases in order to identify the key parameters driving the enforcement action and the economic analysis of the impact of the alleged misbehaviour. Finally, the paper concludes by reviewing how the key facts and findings of the recent enforcement actions

[3] https://www.theguardian.com/news/series/cambridge-analytica-files

contribute to provide evidence in support of new theories of harm based on privacy degradation. We consider those issues in the light of the ongoing debate over whether: i) there is a different problem here; and ii) it is a structural problem (i.e. the characteristics of the market, combined with the incentives of the economic actors, lead to a situation where harm in the form of data exploitation resulting from privacy degradation is not only possible but is a likely outcome in the absence of countervailing factors).

Last but not least, in May 2018 the General Data Protection Regulation ("GDPR") came into effect in the EU[4]. This establishes a strong consent-based, transparent regime for companies that wish to use personal data to improve existing services of provide new ones. The GDPR can potentially change a lot in terms of how personal data is collected and used, at least in Europe. However, it is too early to be able to evaluate what its effects might be. However, we provide at the end a short discussion of what the effects might be, particularly in relation to the potential impact on privacy degradation and the functioning of the data economy, so that future monitoring of its enforcement can focus on specific aspects that are relevant for competition policy and antitrust enforcement.

2. Framework for analysis and theories of harm

In this section, I consider what should be the right economic framework to analyse the new theories of harm, how they link to existing theories of harm, and what are the key aspects to consider in these types of assessments. I conclude by setting out some criteria that could be useful to assess on a case by case whether or not there has been, or is likely to be, consumer harm.

Current theories of harm focus on price effects to the detriment of other aspects

Current theories of harm have developed based on the rise of the Chicago School and its neoclassical, price-centric, analysis of markets[5]. However, economists know now that behaviour, whether short or long term, is driven by other factors as well, and that the consumer suffers from a series of behavioural biases when faced with a supposedly rational

[4] https://www.eugdpr.org/

[5] For a discussion of this, see Chapter 7 of Grunes & Stucke, Big data and Competition Policy, (2016).

decision as an economic agent[6]. Therefore, we know that both the individual preferences and the context ("sensitivities") do matter, as do other service characteristics, such as quality. This is even more so in markets where a service is provided for free (i.e. no monetary fee) in exchange for collecting personal data, as consumers do not act on the basis of a price, but take decision based on other factors. We also know now a bit more about how the data economy works, what are the prevailing business practices, and what ultimately drives economic agents. A recent study by AT Kearney for the GSMA[7] highlights how data driven efficiencies have become dominant for many platforms, driving the way they organise their activities and the way they choose which services and products to launch and into which markets to expand. An analysis of the incentives of businesses is therefore also very important to ascertain whether there could be potential harm.

In order therefore to have an appropriate economic framework, it is important to discuss in more details each of these three aspects.

Consumer side - Consumer preferences

Consumer behaviour is traditionally analysed with reference to the neoclassical economic model, whereby economic agents are considered rationale, and act on the basis of prices which convey all the required information about the product or service in question. However, economists, and policy makers, have now accepted that consumer cannot always take a fully rationale decision[8] or suffer from behavioural biases that lead them to take into account other, environmental, factors into account when taking their economic decision[9].

In the case of privacy, the influence and importance of what can be loosely called the **contextual preferences** (public perception, institutional perception, family and friends' perception) can be determinant in affecting the type of importance to attach to a possible abusive behaviour. For a start, privacy can be considered a type of social good[10]. Its

[6] A good practical illustration of this is set out in the consumer segmentation work done by the Financial Conduct Authority in the UK in relation to financial markets, which has been recently applied to remedies in the current accounts and savings UK markets, see https://www.fca.org.uk/about/promoting-competition

[7] https://www.gsma.com/publicpolicy/the-data-value-chain

[8] For example, the concept of bounded rationality for economic agents, whereby constraints limit the rationality of economic decisions, has been first put forward in 1982 by H.Simon (1982).

[9] The use of behavioural sciences in economics has become today mainstream, thanks also to the work of the R.Thaler from the University of Chicago, who was awarded a Nobel prize for his work in 2017; a good reference site for research in this areas is https://www.behavioraleconomics.com/

[10] See Kasper (2007) for an interesting explanation of how considering privacy as a social good, rather than a kind of private good, can help achieve better privacy policies.

enforcement as a collective right is important as consumers care if the privacy of others is protected, or if violation of others' privacy is sanctioned.

When it comes to the **individual preferences**, the more the contextual preferences are tuned towards protection of privacy, the more likely it is that the individual will also care about privacy.

If you also consider that the opportunity for violating personal privacy have increased massively thanks to digitalisation, the spread of smartphones, and the mass collection of personal data through the internet, then it can be expected that we have both a situation where consumers care about privacy (and its violation) and one where it is likely it will happen given the volume of data generating digital interactions that our society produces every day.

Economic impact

In order to assess the likelihood of consumer harm from data exploitation resulting from privacy degradation, we need to have more than a dislike for the possibility of privacy degradation, and a high likelihood that it will happen. The likely harm must be, ideally, observable and measureable. This matters because even if the collection of personal data is generally disliked as a business practice, the data that is collected is used to generate economic value, either through improved products and services, or through new ones. The likely harm needs therefore to be expressed in a way that can be measured against the benefits that the data collected could be generating[11]. Usually, in an economic assessment we can use data on switching and prices to gauge the impact of certain behaviours on consumers. In zero price markets with low entry barriers and consumers multi-homing, this is not possible, as there is no price and switching as we are used to. We have therefore to come up with a different way of measuring the value of privacy, and therefore the value destruction of privacy degradation.

On the value of privacy, we can of course carry out survey and ask consumers. Sophisticated surveys with discrete choices can derive an implicit value for a good even when users are not faced with prices. However, this can take time and works well if enough

[11] We are avoiding here to discuss the case of privacy being violated to obtain an illegal economic benefit (for example for counterfeiting, online scams etc.) as these are generally dealt with under criminal law.

relevant people is captured by the survey. Another way of doing this is to consider the other side of privacy, i.e. the personal data that is being protected. If we can find a reference value for the underlying data, then we can work with that[12]. Even when a direct reference value cannot be found, one can use different levels of unit value and model the economic impact using those. You then need some criteria or rule that helps you restrict the range of possible outcomes to something that is realistic.

Platform behaviour – Do the incentives to misbehave dominate?

The third element which needs to be considered when assessing whether there has been harm from data exploitation resulting from privacy degradation relates to the business environment where companies operate, and, in particular, to the business models and practices of the data economy.

Not all businesses that collect personal data from the digital interaction of customers on their platform seek to exploit it separately from the service they provide. Netflix, for example, makes great use of the digital data generated by customers interacting with its content platform, but only to provide them with targeted suggestions as to which content is most relevant to them. Similarly, Apple uses the users' data it collects only to improve its services. Such platforms usually engage with consumers through a traditional commercial model, whereby for a subscription fee customers can access the content offerings, be it Netflix videos of Apple's music.
The problem of data exploitation is therefore almost exclusively going to affect digital platforms whose business is directly, and primarily, linked to the collection and exploitation of personal data, and that do not charge customers a fee for their services.

Given the valuations given to companies with access to vast troves of personal data[13], it is clear that the ability to extract and exploit large troves of data is a key competitive advantage in today's economy. Given this, it is logical to infer that such data is the most valuable asset for such companies. It follows that any way of augmenting the value of their data assets, for

[12] For example, a popular app called speedtest.net, which measures the speed of your internet connection for free, was offering on its mobile app the chance to "not share the users data" if the user was willing to pay 0.99 USD.
[13] https://www.cnbc.com/2018/03/20/amazon-just-passed-alphabet-to-become-the-worlds-second-most-valuable-company.html

example by combining it with a different dataset from another source, or expand it geographically to increase volume, becomes very important for such companies.

This new business logic of data-driven efficiencies can underpin innovation and market entry. Scale and scope in data collection, combined with analytical capabilities, give a unique, in some cases unassailable, competitive advantage. Combined with powerful network effects and a tendency for market to tip towards the dominant provider, we have a situation whereby the incentives to push the exploitation of data as much as possible make it the dominant strategy. These businesses have therefore strong incentives to generate data-driven efficiencies and collect as much data as possible, especially of the personal nature.

There are two possible countervailing mechanisms to counter these strong incentives, at least in theory. First, consumer can retaliate towards the provider in a way which harms their business. Traditionally, consumer would switch away from a service or product they do no longer like or consider meet their preferences. In the case of digital services provided for free in exchange for personal data, in most cases multi-homing means customers are unlikely to switch off the service completely, especially if it is used to keep in touch with family and friends (communication services, social networks). It is therefore more likely to disengage, for example by using the platform less. However, here as well the most advanced platforms have developed a system of alerts and notifications that keeps people hooked even when they are not actively engaging with the platform[14]. It is therefore unclear even when one would like to switch off how much one can really switch off. This problem is compounded by a collective action problem, whereby only if all users decide together to switch or stop using the platform then this might happen, but if one user deviates from the action then the network effects quickly unravel the possibility of effective action for the others as well.

Another mechanism that should act as a strong deterrent against privacy degradation by companies collecting personal data is the system of fines and penalties designed to punish those companies that infringe privacy rules. Until recently, it appears that the potential pay-off from the efficiencies generated by increasing the scope and scale of data assets has been of a bigger scale/magnitude compared to the potential fines in most jurisdiction. For example, the maximum fine imposed on Facebook in recent enforcement cases in Europe has been €3 million by the Italian competition and consumer authority (this case is described

[14] In some cases, these systems amount to *nudging* techniques designed to steer the behaviour of the individual towards the desired one, namely interact with the platform.

in more details in the next section). If we consider that, for example, Facebook's revenues in Q1 2018 from mobile advertising, which is fuelled by the users' data, was a whopping $11.97 billion (of which roughly $2.3 billion coming from Europe[15]), then the fines and penalties need to be of a different magnitude altogether if they are to provide for a effective deterrent to exploitative behaviour.

This might change now in Europe thanks to the GDPR, which provides for a maximum fine for a GDPR violation of €20 million or 4 percent of a company's annual global revenue from the year before, whichever is higher. Willingness to consider the maximum penalties in the face of serious infringements will be key in the coming years to how the new regulation works for consumer protection against privacy degradation.

Section conclusions

Existing theories of harm based on price effects are not helpful, especially in the fast moving world of digital markets. Platforms employ business practices tailored to exploit consumers by maximising the amount of personal data they collect. This is especially true for those platforms whose business model is centred on offering free services in exchange for collecting the data of users and using it for purposes other than improving the services they offer, typically advertising.

The lack of a positive monetary price means users behaviour and interaction with these platforms is driven by other aspects, such as quality and the degree of privacy offered. As these other aspects become dominant to understand behaviour and economic welfare in these markets, traditional theories of harm, focused on price effects, cannot alone serve as a useful framework for analysis. Therefore, it is useful to integrate these with some criteria that, based on the discussion above, can help in identifying whether or not harm is likely to occur or has taken place. These are: i) State of consumer preferences – comprising both the individual level and the aggregated, contextual level; ii) Economic welfare considerations – how value is created and distributed among the economic agents; and iii) Incentives to exploit users' personal data, including by degrading their privacy - and any evidence or strong likelihood of retaliation mechanisms for the platforms' users (switching, disengagement).

[15] https://techcrunch.com/2018/04/25/facebook-q1-2018-earnings/

2 Recent enforcement cases and their relevance for theories of harm based on privacy degradation

The established view of the authorities in Europe and the US has been, until recently, that privacy and competition law should not be mixed up, and that the interest of consumers are best served by using dedicated privacy enforcement frameworks. This has been explicitly set out in merger reviews involving the merger of different internet platforms and service providers. For example, in the Google/DoubleClick merger review, the FTC stated at that time that "*[..] Commission lack[s] legal authority to require conditions to this merger that do not relate to antitrust..*"[16]. Similarly, in the Facebook/Whatsup merger case, the EC stated that "*Any privacy-related concerns flowing from the increased concentration of data do not fall within the scope of EU competition law rules […]*"[17].

More recently, however, there have been many cases where authorities have intervened to sanction privacy degradation, chiefly by Facebook, including intervention by competition authorities. These recent cases fall into three broad categories:

I. Cases with a theory of harm involving privacy degradation and data exploitation;
II. Other cases involving National Competition Authorities (NCAs); and
III. Privacy enforcement cases.

I. Cases with a theory of harm involving privacy degradation and data exploitation

Germany – Bundeskartellamt investigation into Facebook's abuse of dominance

Background and rationale for intervention

The *Bundeskartellamt,* the German competition authority, opened a case against Facebook in March 2016[18]. The authority wanted to investigate suspicions that with its specific terms of service on the use of user data, Facebook had abused its dominant position in the market for

[16] https://www.ftc.gov/news-events/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation
[17] http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf
[18] The case is an administrative proceeding rather than a fine proceeding. Administrative proceedings are, in the authority's own words, more appropriate for complex cases that raise difficult legal and economic questions, and for pilot proceedings to clarify the interpretation of the law in a (new) case constellation. The main objective of such proceedings is not to impose a fine but to re-establish pro-competitive conditions as fast as possible. The authority may however decide to initiate a fine proceeding in the case of recurrent abusive behaviour or in cases with a high potential for significant harm; see: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568

social networks. In initiating the proceedings, the authority stated: "*There is an initial suspicion that Facebook's conditions of use are in violation of data protection provisions. Not every law infringement on the part of a dominant company is also relevant under competition law. However, in the case in question Facebook's use of unlawful terms and conditions could represent an abusive imposition of unfair conditions on users. The Bundeskartellamt will examine, among other issues, to what extent a connection exists between the possibly dominant position of the company and the use of such clauses.*"

Basis for intervention

Under German Competition Law, If a dominant company makes the use of its service conditional upon the user granting the company extensive permission to use his or her personal data, this can be taken up by the competition authority as a case of "exploitative business terms". With the provision on exploitative abuses the law aims to protect the opposite market side in a commercial agreement or transaction from being exploited by a dominant company. Such exploitation can take the form of excessive prices (price abuse) or unfair business terms (exploitative business terms). This is designed to ensure that small parties, including individuals, to a commercial agreement or transaction that are contracted by a dominant firm are not made to accept unfair terms and conditions on the basis of the lack of alternative, bargaining power or transparency and clarity.

In particular, the application of data protection principles for the competition law assessment in the current case is considered by the German authority to be backed by the case-law of the German Federal Court of Justice on § 19(1) *Gesetz gegen Wettbewerbsbeschränkungen* (GWB, the German Competition Law). This concerns in particular two decisions by the Federal Court of Justice in which the Court ruled that the general clause of § 19(1) GWB can also be used to establish that a company is using exploitative business terms. The relevant decisions are the rulings in the *VBL Gegenwert II case*[19] and the *Pechstein case*[20].

[19] According to the ruling in the VBL-Gegenwert case, exploitative business terms cannot only be established on the basis of § 19(2) no. 2 GWB and the comparative market concept applied therein, but can also be established on the basis of the general clause of Section 19(1) GWB. This is the case where the business terms are considered a manifestation of market dominance or superior market power and would be deemed inadmissible business terms under the principles of §§ 307 ff. of the German Civil Code; German Federal Court of Justice (Bundesgerichtshof), „VBL-Gegenwert", KZR 61/11, judgment of 16.11.2013, available via http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/list.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=1 2288, § 68.

[20] In the Pechstein case the Court left open whether the business terms used were exploitative under § 19(1) or (2) no. 2 GWB, but demanded an extensive balancing of interests which also took account of constitutionally protected rights. Accordingly, to protect constitutional rights, § 19 GWB must be applied in cases where one contractual party is so powerful that it is practically able to dictate the terms of the contract and the contractual autonomy of the other party is abolished. If, the Court held, in such a case a dominant company

Based on these principles, the *Bundeskartellamt* decided to examine whether Facebook's data processing terms were admissible. In its assessment, the *Bundeskarellamt* includes the principles of the harmonised European data protection rules, in particular the EU General Data Protection Regulation (GDPR), which entered into force in May 2018, but also the 95/46 EC Data Protection Directive, which could be directly applied to cases under § 19(1) GWB.

Preliminary assessment

On 19 December 2017, the *Bundeskartellamt* notified Facebook in writing of its preliminary assessment's results[21]. In it, the authority points to Facebook being dominant on the German marketefor social networks. The authority further holds the view that Facebook is abusing this dominant position by making the use of its social network conditional on it being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account. These third-party sites include firstly services owned by Facebook such as WhatsApp or Instagram, and secondly websites and apps of other operators with embedded Facebook APIs. Andreas Mundt, President of the *Bundeskartellamt*, stated at that time: "*We are mostly concerned about the collection of data outside Facebook's social network and the merging of this data into a user's Facebook account. Via APIs, data are transmitted to Facebook and are collected and processed by Facebook even when a Facebook user visits other websites. This even happens when, for example, a user does not press a "like button" but has called up a site into which such a button is embedded. Users are unaware of this. And from the current state of affairs we are not convinced that users have given their effective consent to Facebook's data tracking and*

disposed of constitutional rights of its contractual partners, the law had to intervene to uphold the protection of such rights. Relevant legal provisions in this regard were, according to the Court, the general clauses under civil law, one of which is § 19 GWB. The Court held that these clauses should be applied with a view to balancing the conflicting positions of the contractual parties in such a way that the constitutional rights of all parties were, as far as possible, maintained. The decision can be found at: http://www.bundesgerichtshof.de/DE/Home/home_node.html;jsessionid=CAFAE8B04B066B211B25725DD2C8B4E5.2_cid294

[21] With the preliminary assessment notice, the *Bundeskartellamt* offers the company a chance to comment on the allegations and provide justification for its conduct or offer possible solutions. Facebook now has the opportunity to comment on the *Bundeskartellamt*'s preliminary assessment notice and provide justifications for its conduct or offer possible solutions. The proceeding is thus now into a second phase of negotiations with Facebook. Possible outcomes are the termination of the case, the offer of commitments by the company or a prohibition by the competition authority. A final decision on the matter was not expected before early summer 2018; see: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2017/19_12_2017_Facebook.html

the merging of data into their Facebook account. The extent and form of data collection violate mandatory European data protection principles."[22]

According to the authority's preliminary assessment, Facebook's offers data-driven products, which rely on the users' personal data and generated content. The value of Facebook's business, as a result, increases when Facebook's users' data collected on its platform can be combined with users' data from other sources. Facebook has therefore, in the German authority's view, an economic incentive to harvest users' data from different sources and combine it. These other, third party sources, can be either Facebook's other platforms (like Instagram and Whastup), or third party's websites. When operating this business model, the authority argue, Facebook, as a dominant company, must consider that its users cannot switch to other social networks. Participation in Facebook's network is conditional on registration and unrestricted approval of its terms of service. Users are given the choice of either accepting the "whole package" or doing without the service. In particular, the German authority argues that in the case of Facebook, the private use of the network by a given individual user is dependent, among other things, on the fact that Facebook can unrestrictedly collect every kind of user data from third sources, attribute it to the user's Facebook account and use it for numerous data processing activities. According to the *Bundeskartellamt*'s preliminary assessment, Facebook's terms of service are at least in this aspect inappropriate and violate data protection provisions to the disadvantage of its users.

In view of the company's dominant position, the authority argues that it can also not be assumed that users effectively consent to this form of data collection and processing. It further adds that users cannot expect data which is generated when they use services other than Facebook to be added to their Facebook account to this extent. Data are already transmitted from websites and apps to Facebook when a user calls them up or installs them, provided they have an embedded API. There are millions of such APIs embedded in German websites and apps. In the authority's assessment, consumers must be given more control over these processes and Facebook needs to provide them with suitable options to effectively limit this collection of data.

Analysis of the theory of harm

There are three components to the German authority's assessment. First, Facebook is considered **dominant** in the market for social networks in Germany. Data from other sources

22 https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html

confirm that, with a market share in excess of 90%[23], Facebook's dominance should not be disputed in this case.

Secondly, that Facebook's has the **incentive to abuse its dominant position**, particularly in regard of the two key business practices under investigation, namely merging users' data from different databases and collection of users' data from third party sources. From Facebook's perspective, the data are of great economic value. The value increases by combining data from different sources, especially for Facebooks' advertising customers. Facebook can use data to optimise its offer and tie more users to its network. The investigation points to three specific effects that are important for the economic assessment of Facebook's dominance and incentives:

- On the users' side, with the merging of the data the "**identity-based network effects**" become stronger, as the companies learns more and more about individual users' behaviour and preferences;
- Consequently, the "**locking-in**" of users on Facebook strengthens, to the detriment of other providers of social networks;
- In addition, with the help of the improved user profiles generated, Facebook is able to improve its targeted advertising offerings, and therefore to become even more attractive to advertisers (**"indirect identity-based network effects"**). In fact, Facebook has become more and more indispensable for advertising customers. This is also reflected in the rapidly increasing advertising turnover Facebook has been able to generate in the past years, particularly mobile advertising[24].

Thirdly, the alleged behaviour by Facebook. Here the *Bundeskartellamt* focus on two important aspects:

- Facebook's alleged infringement rests on the **loss of control** by the user over its privacy rights; in its assessment, the German authority recognised that Facebook offers its services free of charge, and therefore its users do not suffer a direct financial loss from the fact that Facebook might be using exploitative business terms. The damage for the users lies according to the theory of harm in a loss of control: they are no longer able to control how their personal data are used; this, under German privacy law, constitutes an infringement of the user's protected rights in relation to its personal data; the loss of control manifest itself in three different moments:

[23] For example, see: http://www.wordbank.com/blog/social-media/essential-german-social-media-guide/
[24] https://www.statista.com/chart/2496/facebook-revenue-by-segment/

i. **"Off-platform" data collection**: when Facebook collects data from third parties platforms and website (off platform);

ii. **Merging of users' data from third party with own data**: when the data collected is then merged with the users' data collected on Facebook (on platform); Facebook's users are oblivious as to which data from which sources are being merged to develop a detailed profile of them and their online activities. On account of the merging of the data, individual data gain a significance the user cannot foresee; because of Facebook's market power users have no option to avoid the merging of their data, either. Facebook's merging of the data thus also constitutes a violation of the users' constitutionally protected right to informational self-determination;

iii. **When signing up for Facebook** - Facebook's **framing of the consent is such that it leaves to users no choice but to accept all terms and conditions**, given the absence of a clear explanation of what happens if you do not accept (the users' most common and logical assumption being therefore that if you do not accept all terms and conditions then you will not be able to sue the service).

Finally, there has been some discussion as to whether the *Bundeskartellamt*'s Facebook case provides a precedent for other jurisdiction, or whether it is specific to the German Law. While it is true that this case is grounded in German competition and privacy laws and enforcement practices, this does not preclude it from providing a valid reference point for future interventions. Firstly, with the GDPR now in effect, some of the protection of personal data previously afforded in Germany is now available to all European citizens. Secondly, given the increasing public and institutional concerns over the way personal data is being collected, shared and used, it is fair to assume that a higher standard of protection might be warranted going forward given the failure of previous regimes to prevent abuses on a very significant scale.

Microsoft-LinkedIn merger[25]

Background

The parties notified the European Commission on 14 October 2016. Microsoft is a global technology company based in US which develops, licenses, and supports software products, services and devices. Microsoft's products include operating systems for PCs, servers, and

[25] http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=2_M_8124

mobile devices (branded "Windows"), cross-device productivity applications (branded "Office"), video games, as well as cloud-based solutions and online advertising. Microsoft also provides other software solutions, including customer relationship management (branded "Dynamics"), which is a type of software used by businesses to manage their sales, marketing and customer support activities. LinkedIn is a US based company that operates the homonymous Internet-based social networking service that focuses on promoting professional connections. Professional social network services are offered as free of charge basic subscriptions or premium subscriptions. Among premium subscriptions, LinkedIn offers a sales intelligence solution for businesses branded "Sales Navigator." This product grants access to a subset of the entire LinkedIn database that can be purchased by businesses that also buy customer relationship management solutions. LinkedIn also provides recruiting tools and online education courses as well as it offers advertising space to individuals and enterprises.

Assessment of the proposed transaction[26]

A *prima facie* analysis found that the two companies had limited overlap in their products (no significant horizontal effects). So one of the key question became whether there were other, non-horizontal effects that could restrict competition and harm consumers if the transaction was allowed to proceed without any restrictions. The European Commission's investigation focused in particular on three areas: (i) professional social network services, (ii) customer relationship management software solutions, and (iii) online advertising services. I will focus here on the first part, namely the assessment of the proposed transaction in relation to the professional social network services, which is where the EC put forward a theory of harm based on privacy degradation/data exploitation[27].

Market definition and SMP assessment

Firstly, the EC defined a **separate professional social networks (PSN) market** that include LinkedIn to be national in scope within the EU. The EC found LinkedIn to be the main provider by a good margin in most EU markets (80-90% market share), with the exception of Austria, Germany and Poland. It finds that "*the ability (subject to user's consent) to access Outlook users' address books and suggest new LinkedIn connections on this basis may*

[26] http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf

[27] In respect of CRMs, the EC considered that Microsoft is a relatively small player, and it faces strong competitors, such as Salesforce, the clear market leader, Oracle and SAP. The EC concluded that it unlikely that the transaction would enable Microsoft to foreclose these players and eliminate competition in this market. In relation to online advertising, given their very limited combined market share in the EEA, as well as the fragmented nature of the market, the Commission excluded any competition concerns arising from the combination of the parties' online non-search service activities.

enable the merged entity to significantly expand the size of its PSN." It then finds that network effects would reinforce dominance and foreclose competition ("tipping"), and that new entry or multi-homing exert limited constraints.

Non-horizontal issues with the proposed merger

The Commission looked at whether, after the merger, Microsoft could use its strong market position in operating systems (Windows) for personal computers and productivity software (including Outlook, Word, Excel and Power Point) to strengthen LinkedIn's position among professional social networks. While it found no horizontal concerns with the merger due to limited overlap, it had significant concerns linked to different effects (non-horizontal concerns). In particular, the European Commission was concerned that Microsoft would:

- Pre-install LinkedIn on all Windows PCs; and
- Integrate LinkedIn into Microsoft Office and combine, to the extent allowed by contract and applicable privacy laws, LinkedIn's and Microsoft's user databases. This could have been reinforced by shutting out LinkedIn's competitors from access to Microsoft's application programming interfaces (APIs), which they need to interoperate with Microsoft's products and to access user data stored in the Microsoft cloud.

The Commission found that these measures could have significantly enhanced LinkedIn's visibility whilst competing professional social networks could potentially be denied such access. As a result, LinkedIn would have been able to expand its user base and activity in a way that it would not have been able to do absent the merger. In terms of the effects on consumers, the EC was concerned that consumer choice could be directly affected by the merger in two ways:

- **There would be a monopoly with no choice of alternatives** in the market for PSN services; and
- To the extent that these foreclosure effects would lead to the **marginalisation of an existing competitor which offers a greater degree of protection to users** than LinkedIn (or make the entry of any such competitor more difficult), the merger would also have **restricted consumer choice in relation to this important parameter of competition (i.e. privacy)** when choosing PSN. By way of example, the results of the Commission's investigation revealed that, today, in Germany and Austria, Xing seems to offer a greater degree of privacy protection than LinkedIn. In its

assessment, the EC provides thee examples of how XING gives users more control over their privacy to illustrate its point.

In short, the Commission was concerned that the increase in LinkedIn's user base would make it harder for new players to start providing professional social network services in the European Economic Area (EEA). Furthermore, it was concerned that this could have gradually and irreversibly tipped the market towards LinkedIn in Member States where a competitor of LinkedIn currently operates (such as Austria, Germany or Poland).

Decision to approve the merger subject to remedies

On the 6 December 2016, the European Commission approved under the EU Merger Regulation the proposed acquisition. The decision was conditional on compliance with a series of commitments aimed at preserving competition between professional social networks in Europe. In particular, to address the competition concerns identified by the Commission in the PSN services market, Microsoft offered a series of commitments, including:

- Ensuring that PC manufacturers and distributors would be free not to install LinkedIn on Windows and allowing users to remove LinkedIn from Windows should PC manufacturers and distributors decide to preinstall it.
- Allowing competing professional social network service providers to maintain current levels of interoperability with Microsoft's Office suite of products through the so-called Office add-in program and Office application programming interfaces.
- Granting competing professional social network service providers access to "Microsoft Graph", a gateway for software developers. It is used to build applications and services that can, subject to user consent, access data stored in the Microsoft cloud, such as contact information, calendar information, emails, etc. Software developers can potentially use this data to drive subscribers and usage to their professional social networks.

The EC accepted the commitments. These would apply in the EEA for a period of five years, and would be monitored by a trustee. These commitments addressed the competition concerns identified by the Commission, and cleared the way for the EC’s approval of the acquisition.

II. Other cases enforced by NCAs

FTC's investigation into Facebook's compliance with 2011 consent decree

Background

In March 2018 the FTC opened a non-public investigation into whether Facebook, by allowing third parties to access users' data, has broken a 2011 consent decree given by the FTC. Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups. At the end of a year-long investigation, Facebook agreed to settle - though admitted no actual fault - that it "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public". The FTC did not fine Facebook at that time.

The 2011 FTC investigation

The FTC identified a number of instances in which Facebook allegedly made promises that it did not keep when it came to its users' privacy:

- In December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. They didn't warn users that this change was coming, or get their approval in advance.
- Facebook represented that third-party apps that users' installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data – data the apps didn't need.
- Facebook told users they could restrict sharing of data to limited audiences – for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.
- Facebook had a "Verified Apps" program & claimed it certified the security of participating apps. It didn't.
- Facebook promised users that it would not share their personal information with advertisers. It did.
- Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.
- Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn't.

The final settlement barred Facebook from making any further deceptive privacy claims, requires that the company get consumers' approval before it changes the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years. Specifically, under the 2011 settlement, Facebook is:

- Barred from making misrepresentations about the privacy or security of consumers' personal information;
- Required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
- Required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- Required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
- Required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected.

The final settlement also contained standard record-keeping provisions to allow the FTC to monitor compliance with its order.

The 2018 investigation

The 2011 consent decree also required that users be notified explicitly if their data is shared beyond the privacy settings they have configured. Facebook may have violated that portion of the settlement by allowing Aleksandr Kogan, an academic at Cambridge University, to obtain data belonging not only to people who downloaded an app he created, called "thisisyourdigitallife," but also those individuals' friends. The data collected from the app was later passed on to Cambridge Analytica, which reportedly retained it even after telling Facebook it had been deleted.

Violating the consent decree could carry a penalty of $40,000 per violation, so it could result in principle in a hefty fine for Facebook. A final decision is expected during the final quarter of 2018 at the latest.

<u>Italy - Investigation into third party use of Facebook users' data</u>

Background

On the 6th of April 2018, AGCM, the Italian competition and consumer authority, opened an investigation into Facebook's for alleged unfair commercial practices under the Consumer Code. In particular, the AGCM alleges that Facebook has not properly informed its users in relation to the sharing of data with third parties, and that users are unfairly conditioned to give consent when they are browsing other websites, while also providing unwillingly in most cases, information to Facebook.

The AGCM stated that it will examine the information provided when registering to Facebook's platform, with reference to the collection and processing of the user's personal data for commercial purposes, including the data generated from the use of apps belonging to companies of the group and user's access to third parties' websites and apps. In addition, the AGCM will investigate the automatic activation of Facebook's platform for the exchange of user data when the user accesses third parties' websites and apps without consent and the sole right of opt-out. Finally, the AGCM highlighted that Facebook may be conditioning its users to give their consent in an automated and uninformed way.

III. Privacy enforcement cases

In the past two years, there has also been a surge in privacy enforcement cases. Quite a few of those cases were triggered by Facebook's decision to pool Whatsup users' data with its own users' data following the acquisition of the communication platform in 2014, others have been more recently triggered by the Cambridge Analytica scandal.

The EC fine of Facebook/Whatsup

Following its acquisition by Facebook in August 2016, WhatsApp published a new version of its terms of service and privacy policy allowing the sharing of its users' data with Facebook. This was done despite a previous public statement in which the company had said that it would not be sharing user information with Facebook. In May 2017, the European Commission fined Facebook €110m for providing misleading information during the merger control review.

National enforcement cases

In October 2016, data protection authorities gathered in the Article 29 Working Party (WP29) expressed "serious concerns" about how information on the updated terms of service and privacy policy had been given to users and, consequently, about the validity of their consent.

WP29 urged WhastApp “not to proceed with the sharing of users’ data” with Facebook until “appropriate legal protections can be assured”. In October 2017, WP29 reiterated its concerns. However, it is for national DPAs, and not for WP29, to enforce the national laws implementing EU data protection rules. Several DPAs have already taken action against WhatsApp.

Belgium

In Belgium, the Belgian Privacy Commission issued in 2017 a set of recommendations to the Facebook Group about its tracking of users and non-users of Facebook through cookies, social plug-ins and pixels. The Belgian Privacy Commission considered that Facebook acted in non-compliance with both Belgian and EU data protection law as regards the tracking of both users and non-users of Facebook through cookies, social plug-ins and pixels. In particular the legal requirements regarding consent, fairness, transparency and proportionality are not met, amongst others due to the shortcomings in the information that Facebook communicates to data subjects and the inadequacy of the choices that Facebook offers data subjects.

The Belgian Privacy Commission further considers that the collection of personal data by Facebook using cookies, social plug-ins and pixels is excessive in several circumstances. The Privacy Commission sought judicial enforcement of its recommendations before the Court of First Instance of Brussels. The Court ruled in favour of the Belgian Privacy Commission in February 2018. An appeal is now possible.

France

The investigations conducted by the CNIL in 2017 found several infringements of the French Data Protection Act by Facebook:

- Proceed to a compilation of all the information it has on account holders to display targeted advertising without having a legal bases. If the users have means to control the display of targeted advertising, they do not consent to the massive compilation of their data and cannot object to this compilation when creating account or a posteriori.
- Proceed to an unfair tracking of internet users via the “datr,” cookie. The cookie banner and the mention of information collected "on and outside Facebook” does not allow them to clearly understand that their data are systematically collected as soon as they navigate on a third site including a social plug in. Therefore, the massive data collection carried out via the “datr” cookie, is unfair due to the lack of clear and precise information.

- Concerning other infringements, it considered that Facebook:
- Did not provide direct information to internet users concerning their rights and the use that will be made of their data, in particular on registration form;
- Collected sensitive data of the users without obtaining their explicit consent. Indeed, no specific information on the sensitive nature of the data is provided to users when they complete their profiles with such data;
- By using the web browser settings, did not allow users to validly oppose to cookies placed on their terminal equipment;
- Did not demonstrate the need to retain the entirety of IP addresses of users all along the life of their account.

The CNIL fined Facebook €150,000.

Germany

The Hamburg's Data Protection Authority (DPA) issued on September 27, 2016 an administrative order against the mass synchronisation of data between Facebook and WhatsApp. With immediate effect, Facebook was ordered to stop collecting and storing the data of German WhatsApp users and to delete all data that had already been forwarded by WhatsApp.

Italy

The AGCM announced on 12 May 2017 that it had closed two investigations concerning alleged *infringements of the italian Consumer Code, by WhatsApp Inc., and had issued a* ***fine of €3*** **million** for unfair commercial practices. In particular, the AGCM found that WhatsApp had *de facto* **forced its customers to accept the new terms of use, including the provision to share their personal data with Facebook**, Inc. by inducing them to believe that without granting such consent they would not be able to use the service anymore. The AGCM stated that WhatsApp **had placed excessive emphasis on the need to accept the new conditions or lose the service**, had **provided inadequate information on the possibility to deny consent**, pre-selected an opt-in, and made it difficult to opt-out once the terms of use had been accepted in full.

The Netherlands

In the Netherlands, the *Autoriteit Persoonsgegevens,* the Dutch Data Protection Authority, after an investigation, concluded that Facebook violates Dutch data protection law. In particular, the company gives users insufficient information about the use of their personal data, it uses sensitive personal data from users without their explicit consent. For example, data relating to sexual preferences were used to show targeted advertisements. The Facebook Group has made changes to end the use of this type of data for this latter purpose. The Dutch DPA is currently assessing whether the other violations have stopped. If that is not the case, the Dutch DPA may decide to issue a sanction. The case is still ongoing.

Spain

In September 2017, AEPD, the Spanish DPA, fined Facebook **€1.2 million** for **breaking privacy rules on multiple counts** over the way it uses people's personal data for advertising purposes. Specifically, the AEPD singled out three infringements: i) the way Facebook collects data on people's ideologies and religious beliefs, sex and personal tastes (sensitive personal data) - from its own services and those of third parties - without clearly telling its users what it will do with this information; ii) The fact that **Facebook did not get properly informed consent** from users before exploiting this information; and iii) the fact that the company **violated laws by not deleting data that was no longer useful for the reasons it was collected**. Under EU law, "personal data" means "any information relating to an identified or identifiable natural person," so **people's "likes" would qualify as personal data**.

The Spanish regulator's crackdown follows coordination with agencies in other countries, namely France (which fined Facebook €150,000 earlier in 2017), Belgium, the Netherlands and Germany.

Other countries

In the past months, in the wake of the Cambridge Analitica scandal involving Facebook and the sharing of data with third parties, other countries have launched investigations into Facebook's privacy practices. These include the UK[28], Canada[29], Australia[30] and New Zealand[31].

[28] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/
[29] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180320/
[30] https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica
[31] https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-facebook-must-comply-with-nz-privacy-act/

3 Conclusions

A preliminary survey or recent cases highlights that there is a new theory of harm which is being put forward that is based on privacy degradation. The German's *Bundeskartellamt* investigation into Facebook provides for the most compelling articulation of this to date. It sets out some interesting points in relation to two key aspects, namely Facebook's dominance in the market for social networks, and its behaviour in relation to the treatment of its users' personal data:

- The harm relates to the practice of collecting data on other sites and platforms ("**off-platform collection**") and the **sharing of data with third parties**; no harm is alleged in respect of data collected on its own platform and used to improve services for its own users;
- Facebook, as dominant company in social networks markets, has the ability to put in place harmful behaviour; its dominance is reinforced by the misbehaviour as this increased **direct and indirect identity-based network effects**, and reinforces **lock in** effects for both users and advertisers, to the point where the market tips in its favour, making market entry an unlikely strategy for would-be competitors; and
- Facebook is allegedly at fault also for its **framing of the service agreement** – users are left with the choice between accepting all the terms and conditions, or not participating in the platform (**"all or nothing framing"**).

In the Microsoft/LinkedIn merger case, the European Commission put forward a theory of harm that also had a component based on privacy degradation. In particular, the EC was concerned that the merger would reduce choice for consumers, and, in doing so, **might end up marginalising in particular those competitors that offer better privacy conditions to its users**. In this specific case, the evidence in support of this was provided by a German professional social network platform XING, which offered better privacy settings to its users compared to those offered by LinkedIn.

Finally, the enforcement actions taken by information commissioners and privacy watchdogs are also relevant. These enquiries add evidence to the theory that some practice are acceptable (on-platform data collection and own use), but some others need strong boundaries and consent (framing of service agreement, sharing with third parties and off-platform data collection).

All these cases, cumulatively, provide for a credible theory of harm, at least in theory. This is supported also by the evidence showing a lack of privacy compliance culture, a set of economic incentives stacked in favour of data exploitation, and a lack of credible retaliation mechanisms and deterrents.

So far, Facebook in particular has had some major failures in protecting the privacy of its users. In the major occasions that Facebook has made wholesale changes to its privacy T&Cs, it has ended up giving itself the right to collect more data from the user and, most crucially, making it more widely available publicly even when the user might have actively deselected such option. The FTC's 2011 consent order that followed its investigation is, in that respect, quite striking, in that it identifies many different circumstances where Facebook lied in respect of its privacy policies. Similarly, the decision to merge the data of users from WhatsApp with its own data, going against its own promise to the European Commission not to do that, speaks volume of what drives the platform's behaviour. The potential commercial benefit from merging personal data from different sources clearly outweighed any potential drawback, including regulatory intervention by privacy regulators. This also points to a serious lack of compliance culture at those times inside the organisation when it came to privacy. It is quite astonishing that changes to key terms and conditions for hundreds of millions of users do not appear to have passed a "fit for privacy" test before being rolled out, despite being fur sure a major project taking months to prepare and involving a lot of people at all levels in the organisation. The problem has been made worst by the lack of credible retaliation mechanisms from users that could hurt the company financially. Finally, also the fines designed to deter breaches of users' privacy seem to have so far had little power in preventing misbehaviour.

Potential effects of the GDPR and other, similar, privacy regimes based on functional consent, transparency and effective enforcement

With the GDPR in Europe and other, similar, consent-based privacy regimes based on transparency, consumer empowerment and effective enforcement, the overall picture might change due to the possible impact of such privacy regimes.

On one side, the GDPR is akin to a supply side shock, with the potential to affect significantly the behaviour of consumers in relation to privacy, and as a result the supply of data to platforms and service providers. This means, in practice, that such regimes will affect

the supply of data, for example by making it more difficult to collect and process data, especially from third parties. This in itself would mean a major change given the widespread practices of collecting users' data via third parties and by using cookies. To some extent, the next 12-18 months might reveal much about how consumers, businesses and regulators interact with the GDPR framework, and therefore whether markets and actors adapt in order to keep data flowing to those that make the best use of it and can innovate. There is however much room for discretion in the application of general, principle based regime like the GDPR, so we are likely to see many different behaviours co-exist, and some un-even enforcement action. This might complicate the overall assessment, and require further fine-tuning in the future should the supply condition for data deteriorate significantly.

Another important potential impact of the GDPR and similar regime could be that, given the high burden of compliance it imposes, only the bigger companies are in effect able to comply effectively. This would tip digital markets further in favour of large incumbents. Indeed, Kasper (2007) observes that tight privacy regimes with high compliance standards could also be detrimental for new entry, as consumers are likely to trust existing providers that already handle their data and are known to them, rather than new companies seeking access to their data.

Maybe the most important likely effect, at least in the short-term, might result from the new maximum fines that the GDPR allows to impose (i.e. up to 4 percent of turnover or €20 million, whichever is the highest). Provided there is a willingness to apply the maximum fines in serious cases, this could provide for a far more effective deterrent to misbehaviour, and in effect keep the behaviour of collectors of large quantity of personal data in check. Again, the coming 12-18 months will shed lights on whether this is going to be the case or not. Without such an effective deterrent, the incentives to misbehave, and the payoff from abusing privacy, are likely to remain in favour of privacy degradation and data exploitation for the time being for those businesses that depend primarily on the collection and analysis of large troves of personal data.

References

- Bundeskartellamt, Investigation into Facebook data gathering of its users, http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html
- Campbell, J. D., Goldfarb, A. and Tucker, C. E., Privacy Regulation and Market Structure, Journal of Economics & Management Strategy, Vol. 24, Issue 1, pp. 47-73, 2015
- European Commission, DG Competition, Case M.8124 – Microsoft / LinkedIn, 6 December 2012, http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf
- European commission, DG Competition, Case No COMP/M.7217 - FACEBOOK/ WHATSAPP, 3 October 2014, http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf
- Federal Trade Commission, Google/DoubleClick, 20 December 2007, https://www.ftc.gov/news-events/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation
- GSMA, The Data Value Chain, May 2018, https://www.gsma.com/publicpolicy/the-data-value-chain
- Kasper, D.V.S., Privacy as a Social Good, Social Thought & Research, Vol. 28, Social "Movements", pp. 165-189, 2007
- Kerber, W., Competition, Innovation, and Competition Law: Dissecting the Interplay, Joint Discussion Paper, Series in Economics, by the Universities of Aachen, Gießen, Göttingen, Kassel, Marburg and Siegen, 42-2017
- Prufery, J., and Schottmullerz, C., Competing with Big Data, September 29, 2017
- Simon, H. A., Models of bounded rationality. Cambridge, MA: MIT Press, 1982
- Stucke, M. and Grunes, A., Big Data and Competition Policy, Oxford University Press, 2016
- Which?, Control, Alt or Delete?, Policy Report, June 2018, https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report