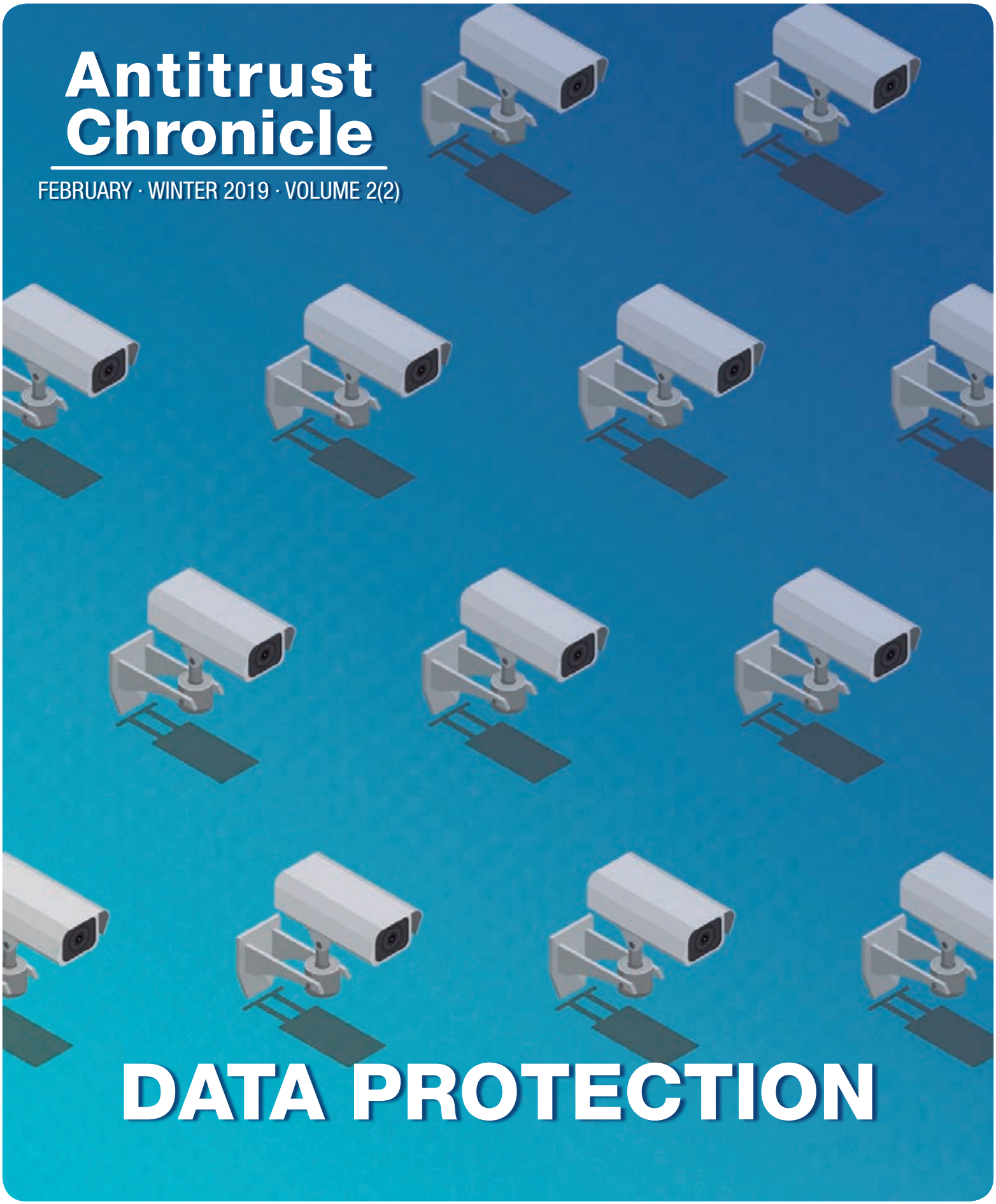
Antitrust Chronicle

FEBRUARY · WINTER 2019 · VOLUME 2(2)



DATA PROTECTION

CPI COMPETITION POLICY INTERNATIONAL

TABLE OF CONTENTS

LETTER FROM THE EDITOR

Dear Readers,

For the second CPI Antitrust Chronicle for February 2019, we turn to a very "spannendes Thema"…the intersection of data protection and antitrust laws. This is a subject that has been "intensiv diskutiert," especially after the recent, highly anticipated, news from Germany's Bundeskartellamt in its Facebook ruling. We have a great group of articles that discuss this recent decision in detail and its possible ramifications. In addition, we have contributions from the U.S. and Brazil.

Some authors argue that "privacy, data protection, and competition law originate from the same creative energy," and put forward that competition and data protection laws can be harmoniously enforced. Some authors take a more cautious approach. Are new precedents being set? Are we starting to see more or less convergence or divergence in enforcement on both sides of the Atlantic?

We are pleased to open this month's Chronicle with a CPI Talks interview with Covington & Burling partner and former Commissioner of the FTC, Terrell McSweeny. In addition, this edition of the Chronicle features articles from Giovanni Buttarelli, European Data Protection Supervisor; Maureen Ohlhausen, partner at Baker Botts and former Acting Chairman and Commissioner of the FTC; and Vinicius Marques de Carvalho, former President of the Brazilian Administrative Council for Economic Defense – CADE, among other notable authors.

Lastly, please take the opportunity to visit the CPI website and listen to our selection of Chronicle articles in audio form. This is a convenient way for our readers to keep up with our recent and past articles on the go, in the gym, or at the beach.

As always, thank you to our great panel of authors.

Sincerely,

CPI Team

SUMMARIES

SUMMARIES

WHAT'S NEXT?

For March 2019, we will feature Chronicles focused on issues related to (1) **LeadershIP EU**; and (2) **China – Year of the Pig**.

ANNOUNCEMENTS

CPI wants to hear from our subscribers. In 2019, we will be reaching out to members of our community for your feedback and ideas. Let us know what you want (or don't want) to see, at: antitrustchronicle@competitionpolicyinternational.com.

CPI ANTITRUST CHRONICLES April 2019

For April 2019, we will feature Chronicles focused on issues related to (1) **Public Procurement**; and (2) **Online Advertising**.

Contributions to the Antitrust Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI Antitrust Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden ( ) with the subject line "Antitrust Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers on any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

CPI TALKS...

...With Terrell McSweeny

In this month's edition of CPI Talks… we have the pleasure of speaking with Terrell McSweeny. Ms. McSweeny is a partner at Covington & Burling LLP, a former Commissioner of the Federal Trade Commission, and a distinguished fellow at Georgetown Law's Institute for Technology Law & Policy. Additionally, she has held senior appointments in the White House, Department of Justice, and the U.S. Senate.

Thank you, Ms. McSweeny, for sharing your time for this interview with CPI.

1. **There is an international ongoing debate on the ways in which competition, data protection, and consumer protection laws interact in the digital economy. Some argue that there is an ethical imperative to meet this challenge and that strong competition enforcement could render data protection rules more effective by facilitating consumer choice. At the other end of the spectrum, others claim that privacy is simply not an antitrust issue. How can we strike the right balance?**

Competition regulators around the world are actively assessing the state of antitrust law and whether technological change requires adjustment to competition frameworks.

In the digital economy we can expect data protection, consumer protection, and competition frameworks to interact with each other to a certain extent. At the same time, it is important to understand that these frameworks are not designed to address the same issues. In some cases, they may be in tension with one another. One the one hand, a competition enforcer may wish to facilitate access to data to alleviate competition concerns. But such access may raise privacy concerns if the data includes personal information. On the other hand, privacy and consumer protection frameworks that allow consumers to easily move their personal data may alter the competitive significance of data by lowering barriers to entry. Striking the right balance depends on thoughtful case-by-case analysis of the facts.

2. **How should we coordinate antitrust cases involving data protection matters with data protection authorities – will there be some sort of institutionalized cooperation, or rather a cooperation on a case-by-case basis? And, how can the case-by-case approach, normally required in dominance investigations, ensure a cohesive data protection policy that addresses industry-wide practices?**

In general, competition agencies should be careful of straying too far into gray zones at the intersection of antitrust law and other legal frameworks. The objectives of these frameworks are not the same and may not always be aligned. If privacy is a dimension of competition in a market before a competition enforcer, then it may be appropriate for the authority to investigate whether there are effects that flow from a loss of that competition. However, competition agencies should avoid picking up the mantle of privacy and consumer protection enforcers. It is important for agencies with subject matter expertise to interpret the laws they enforce.

3. **Can competition problems in the area of data protection and antitrust still be solved sufficiently with structural remedies (as often preferred by competition authorities) or do competition authorities need to pivot to behavioral remedies, also to enable better and faster adaptation to changing circumstances?**

Both U.S. competition agencies have expressed preferences for structural remedies to address harms to the competitive process – though they may resort to behavioral remedies such as licensing in certain circumstances. Depending on the type of data involved, privacy regulations may make behavioral remedies more challenging for competition enforcers.

4. **Should market-dominant undertakings that generate/gather a vast amount of personal and meta data (e.g. Facebook/Twitter in social media; Google in online search; comparison and other ecommerce platforms; Amazon acting as retailer as well as platform for other retailers) be obliged to grant access to their databases to competitors in order to generate a level playing field and/or to counter tipping effects? Are big tech companies essential infrastructures in this regard? If they're not, should we define what an essential facility is differently so as to cover them? Or should we oblige them to grant access to their databases without considering them an essential facility?**

There is no question that data is important in the digital economy. But the value of data depends on the facts. For example, some data are public or can be obtained for a fairly nominal cost. The value of data can also change over time. Data that is old data may grow stale and have less value. Further, data can be non-rivalrous, meaning that the same data can be used by multiple competitors. Such data is not essential. But other data is proprietary and can operate as a barrier to entry. Of course, even proprietary data may not raise competition concerns if others can obtain substitutable data. Generally, the nature, not the volume, of data will determine its competitive significance. Antitrust agencies have proven relatively capable of addressing competition issues around data after careful analysis of its context. Commenters at recent FTC hearings on these topics have expressed a general agreement that simply investing in, or acquiring large quantities of, data is not a cognizable antitrust harm and that requiring a company to provide competitors and new entrants access to data may adversely impact investment and innovation incentives.

It is important for competition enforcers considering these questions to examine whether multi-homing, interoperability, and relatively low barriers to entry in online markets are facilitating competition and innovation with established platforms.

5. **Do you believe that antitrust remedies can properly address data protection concerns? If yes, which remedies can you envision using? And, isn't it necessary to show that antitrust remedies can better address these concerns than dedicated regulations, before applying them? Why would that be the case?**

As I discussed above, data protection frameworks are designed to address the relatively complex question of how much control people should have over their data in a digital economy. They balance a number of aspects of data policy such as choice, transparency, control, access, portability, and correction. Competition tools are limited in addressing many of these issues – and may even be in tension with them.

THIS IS NOT AN ARTICLE ON DATA PROTECTION AND COMPETITION LAW

Ceci n'est pas un article sur la protection des données et le droit de la concurrence.

BY GIOVANNI BUTTARELLI[1]

1 European Data Protection Supervisor.

I. SETTING THE RIGHT *AMBIENCE*

Data protection, privacy, and competition have for a long time acted as if they did not originate from the same creative energy. Protection of the private realm was defined back in 1890 as the foundation of individual freedom in the modern age.[2] It comes as no surprise that the father of privacy, Louis Brandeis, was also so assertive in defending the role of antitrust in ensuring the conditions for democracy and preventing any private entities from having more power than the law.

As much as antitrust and antimonopoly, privacy concerns the protection of those realms which allow human beings to meaningfully exercise their rights and freedoms. As much as in privacy and data protection, there will hardly be any meaningful exercise of freedoms and rights if private actors grow so big as to control information, decisions, knowledge, change, and to ultimately determine the course of disinformation, ignorance, stagnation.

The enforcement of data protection is first of all in the hands of data protection authorities. This *obiter dictum* did not and should not impede that authorities active in the enforcement of other areas of law could base their analysis on privacy and data protection. We are living in a time when we urgently need to get back to the heart of privacy and competition laws to understand how closely they are intertwined and how much they could support each other in tackling some of biggest challenges of today's world.

By postponing a full analysis to a comprehensive Opinion which I will adopt by the end of the year, this piece will comment on the recent decision by the German federal antitrust authority, encourage further convergence of policy goals, and provide personal insights into the near future.

II. A LONG-AWAITED RESULT

The German Federal Cartel Office ("FCO") has recently imposed restrictions on Facebook in their processing of users' data.

The decision found Facebook's terms of service and the manner and the extent to which it collects and uses data "in violation of the European data protection rules to the detriment of users."[3] Facebook's practice of unrestrictedly collecting users' data from different data sources, namely third-party websites and Facebook-owned services, combining and assigning them to an account without the user's valid consent is defined as an exploitative abuse under competition law. Competition law should ensure that consumers can enjoy free and meaningful choice and a decent level of innovation. In the particular case of this decision, the violation of personal data triggers a big problem for competitive markets. All companies in the digital information ecosystem that rely on tracking, profiling, and targeting should be on notice.[4]

The FCO's order represents the culmination of years of crucial discussions, both at the EU and national level, on how to coherently face the challenges of the digital ecosystem. This decision is the first of its kind to, finally, integrate data protection implications into the antitrust remit. Judging from the information publicly available, European data protection provisions are deemed to be a standard for examining exploitative abuses.

While the European Court of Justice ("ECJ") has ruled in *Asnef-Equifax*[5] that any issues relating to the sensitivity of personal data are not, *as such*, a matter for competition law, further consensus should be built on the fact that there is no legal obstacle either in the EU legal framework or in the ECJ case-law to including data protection standards in a competition analysis assessment. This argument was acknowledged in the Joint Report that the French and the German Competitions Authorities issued in 2016.[6]

2 L. D. Brandeis & S. D. Warren, "The Right to Privacy," Harvard Law Review, 1890.

3 Press release "Bunderskartellamt prohibits Facebook from combining users' data from different sources," Bonn, February 7, 2019 available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

4 G. Buttarelli, blog post "Big step towards coherent enforcement in the digital economy," February 7, 2019.

5 Judgment of the Court (Third Chamber) of November 23, 2006, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v. Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, C-238/05.

6 Autorité de la concurrence de la Concurrence, Bundeskartellamt, "Competition Law and Data," May 10, 2016 p. 23.

The FCO also went the extra-mile, by imposing – as it would be legitimate to expect in cases where a big friction with data protection exists – pure data protection remedies. I wonder if this aspect of the decision could give some hints for future reflection on a possible unique regulator, responsible for digital markets.

The decision does not prescribe any fines and is issued at a national level. Overall, however, it has a pioneering potential and it marks an important step in looking at data protection as a benchmark for competition enforcement analysis purposes. After all, the assessment performed under EU data protection law could not occur without the cooperation of the data protection agencies, something we have been intensively advocating at the European Data Protection Supervisor ("EDPS").

III. OSMOSIS OF POLICY GOALS

There is no real consensus over how synergies between privacy, data protection, and competition should be explored and pursued.

Some claim that the approach of mutual inclusion into each other's goals would stigmatize that data protection needs to resort competition law in order to achieve its purposes. Conversely, others fear that this osmosis of goals would "enslave" competition law to issues falling outside its remit.

I disagree with these claims for two fundamental reasons. First, recognizing that the violations of data protection standards can be a benchmark for assessing competition – relevant conduct has very little to do with recognizing the supremacy of one policy tool over the other. On the contrary, it means that authorities, meaning governments and states, are keen to adjusting their operative tools reality, and to modernizing their response to a world which is in continuous transition. Short innovation cycles also mean a short time for officials and operators to "understand" what is happening. Exchange of expertise between regulators can offer support in this regard.

Second, the data protection toolbox is now more powerful than ever. The EU legislator has actually been inspired by the EU competition system when designing, for example, fines and new enforcement instruments. This is not the end of the story. The EU data protection reform has carefully considered the implications for markets and competitiveness, and it has provided for "scalable obligations" in the EU General Data Protection Regulation ("GDPR"). I would not shout out in scandal if competition law could likewise show its full openness to understanding and unveiling the implications that control over data can have in digital markets.

I am hopeful that the FCO's decision, in its inherent ambition of aligning different policy goals, could set an important precedent to be considered by the European Union at a large.

IV. WHAT IS AT STAKE

So as the title of this contribution implies, much of the analysis should actually move on from being only focused on data. There are broad questions of choice and fairness in the digital economy.

It is often claimed that policy-makers and enforcers only get to understand complex dynamics and problems with unfortunate delay. Bureaucracy takes time, after all. Nevertheless, I feel we should urgently accelerate our understanding of the real harms that people suffer online. At the EDPS, we have been committed to unveiling the covert perils of a big data environment by looking beyond data as such.

All eyes are on Europe and on its leading by example in data protection. In a moment where the whole world is now, finally, acknowledging the importance of high personal data protection standards, and its literally changing legislation and conversations around the GDPR it is imperative that we take the debate a step further. Should we stick to data only, we would run the risk of failing to grasp the bigger picture.

Tech titans´ "way of being" reveals a far more complex world where the actual "holy grail" of their brokerage is our *entire existence*. A very small number of giant companies have emerged as effective informational gatekeepers of the content which most people consume.[7]

As the protection of personal data is instrumental to the protection of other rights and freedoms, so is the harm to personal data.

Our feelings, emotions, uncertainties, and hopes for the future are caught in a process which is likely to benefit – in the long run – only

7 EDPS Opinion on "Online manipulation and personal data," March 19, 2018.

one part of the transaction. Our opinions, civic and political engagement, and ultimately our ability to think independently and as rational human beings are subject to constant surveillance and manipulation, whose details we know little of, any at all. And on which the digital person seems have zero chances of intervention.

V. OPEN QUESTIONS FOR OPEN PROBLEMS

Control over personal data can lead to control over human beings. In this regard, there are legitimate concerns of a possible *vulnus* on our democracies at a large.

Competition law has its historical roots in preserving the democratic assets and outlook of societies. In the EU, it is also a means for the functioning of the internal market. Digital citizens deserve tools which encapsulate a proper response to reality. Competition should go back to its roots and protect those assets and outlook now in danger.

In exploitative abuses, many important issues remain open. How to forge theories of harm capable of unmasking the abuses occurring online? Part of the debate should focus on the pivotal specificity of our digital economy, meaning the frequent absence of a price paid by the consumer. The so-called zero price markets, to which abundant literature from both sides of the Atlantic and beyond devoted careful attention, are still a mystery to be fully unveiled. We need a metrics and a reliable methodology to assess what the real cost of non-monetary pricing is. Degradation of privacy and data protections risks capturing only one part of the overall picture.

Much more is still to be explored, such as how to measure and give meaning to the different and wider forms of nuisance or disservice delivered to users: attention's seizure and addiction, advertising saturation. This has much to with "excessive" exposure and interference with our private lives, or if you want, pricing. Starting with the comprehension of the harm may even help with market definition. Framing the relevant market as to more broadly encompass those services competing for our time or attention could represent an intelligent approach to market definition in today's digital ecosystem.[8]

EU competition law has the right tools to rebalance trading conditions and restore their fairness. As postulated by the Treaties, EU competition law should tackle both exclusionary and exploitative abuses, something that enforcement seems to have overlooked, ending up focusing almost only on exclusionary effects.

Equal attention should be turned to exclusionary abuses. Data-fueled tech giants have the capability of gathering all sources of information and evidence over potential competitors and to detect this competition well in advance. The result is that either they buy their competition or try to squash it. This form of "intelligence" that tech titans conduct on potential competitors may dramatically lead to boycotts of ethical forms of innovation, based on the respect and enhancement of fundamental rights.

Many of the considerations in this section are applicable *mutatis mutandis* to merger control.

VI. A VISION FOR THE NEAR FUTURE

The EDPS is pleased to have initiated the debate, at the EU institutional level, on the convergence of issues in the digital economy and on alignment of responses.[9]

During my mandate, I have brought this endeavor further, by calling for the establishment of a Digital Clearinghouse were regulators and authorities could sit together and explore synergies in their respective fields of action.[10] In more detail, the Digital Clearinghouse is the first network of its kind to bring together all regulators responsible for the enforcement of laws in the digital ecosystem. At present, it includes competition, data protection, consumer protection and electoral regulators and authorities from Europe and beyond. The network had four meetings so far between 2017 and 2018, and we expect even more in the near future. Discussions in the forum are meant to support a convergence in

8 Tim Wu, "Blind Spot: The Attention Economy and the Law," Columbia Law School, 2017, where the author proposes an "attentional version of the SSNIP test," to determine "how consumers might react to a small but significant and non-transitory increase in the advertising load for a given product," p.29.

9 EDPS Preliminary Opinion on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy," March 26, 2014.

10 EDPS Opinion on "Coherent enforcement of fundamental rights in the age of Big Data," September 26, 2016.

the understanding of this complex world.

The Digital Clearinghouse is one important example of the type of dialogue we need.

Enhanced cooperation could also take the form of a dedicated inter-institutional mechanism to facilitate convergence on substance. The European data protection authorities sitting in the EDPB have offered their expertise in support of competition enforcement in August 2018, on the occasion of commenting on the impact that economic concentration has on rights and freedoms.[11]

The potential of a unique, digital regulator, responsible for a coherent and linear monitoring of our markets and societies in the digital age is also tempting in terms of resources efficiencies and likely linearity of results.

I intend to set out a broader vision this year for achieving all this.

11 EDPB Statement on the data protection impacts of economic concentration, August 27, 2018, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf.

PRIVACY AND COMPETITION: FRIENDS, FOES, OR FRENEMIES?

BY MAUREEN K. OHLHAUSEN[1]

1 Partner, Baker Botts LLP. The author would like to thank Brian Jacobsmeyer for his research assistance.

I. INTRODUCTION

The debate about the future of data rich tech companies has reached a fever pitch in the European Union ("EU")[2] and, to a slightly lesser extent, the United States, with some voices calling for changes to consumer privacy law, competition law, or both to address perceived concerns. The desire to impose increased restrictions on data collection, usage, and sharing in the name of consumer privacy is manifest in Europe's adoption of the General Data Protection Regulation ("GDPR").[3] The regulatory impulse is not limited to changing consumer privacy law, however, and some have advocated using competition law to impose new controls and obligations on entities that collect consumer data. In fact, there has already been some melding of consumer privacy and competition concerns in data regulation itself. For instance, the GDPR mandates data portability to allow consumers to move their data among competing entities and thereby avoid "lock in" that may otherwise give current strong players an ongoing competitive advantage. Competition concerns reflect the fact that data about, or generated by, consumers can be a valuable asset. For example, The Economist magazine famously characterized data as the new oil.[4] Reflecting this view, some have called data an essential facility and have advocated using competition law to force big tech companies to share consumer data because of its utility as an asset today and as an essential input into new products and services tomorrow.

This article will explore the challenges and limits to these theories and the tension they create between reducing and widening access to consumer data. Can privacy and competition values live in harmony as friends, will some of these proposals make them enemies, or is it a bit of both?

II. GDPR, DATA BROKERS, AND DATA PORTABILITY

The GDPR, which took effect in May 2018, generally applies to companies processing the personal data of residents of the EU. The GDPR's definition of "personal data" is broad, covering any information that can directly or indirectly identify a person, such as a name, identification number, location data, or online identifier. The regulation also has a broad geographical sweep and applies to entities outside the EU that offer goods or services to EU citizens (regardless of whether payment is required) or monitor behavior that takes place within the EU.

The GDPR's fundamental requirements are that personal data be processed lawfully, fairly, and in a transparent manner. The regulation states that personal data may only be collected for specified, explicit, and legitimate purposes and not be further processed in a manner incompatible with those purposes. It also limits data collection to what is necessary for the purposes of processing. Personal data must also be accurate and kept up to date but retained for no longer than necessary. Companies must also ensure the integrity and confidentiality of the personal data they collect, including against unauthorized or unlawful processing and against accidental loss, destruction, or damage. The entity that controls personal data is responsible for, and must be able to demonstrate, compliance with the GDPR's requirements.

The GDPR further states that processing is lawful only under certain conditions, with a prime example being when the data subject has given consent freely and in a specific, informed, and unambiguous manner. For example, the request for consent must be in an intelligible and easily accessible form and use clear and plain language.[5] Moreover, the entity controlling the personal data must be able to demonstrate that consent, and individuals can withdraw consent at any time.

Consent is not required in all situations, however, such as in connection with performing a contract with a person. The GDPR also permits processing for the data controller's legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Legitimate interest is not based on a particular purpose, like performing a contract with the individual, and it could in principle permit processing for a wide variety of purposes. The GDPR does not provide a detailed list of legitimate interests, although it offers the examples of fraud prevention, network and information security, and public security. It also states that processing employee or client data, direct marketing, or administrative transfers within a group of companies may indicate a legitimate interest.

---

2 See, e.g. a 2/1/19 tweet by Giovanni Butarelli, European Data Protection Supervisor, that said, "1865 President Lincoln abolished slavery. We now face the challenge of abolishing digital servitude – where people are mined for their data, and served back personalised information in order to induce behaviours that benefit a few powerful players #CPDP2019." Putting aside the question of the appropriateness of the comparison, the statement illustrates the intensity of European privacy regulators' sentiment about data.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

4 "The World's Most Valuable Resource," The Economist (London, May 6, 2017).

5 For example, on January 21, 2019, the French National Data Protection Commission ("CNIL") imposed a penalty of 50 million euros against Google LLC, under GDPR for lack of transparency, inadequate information, and lack of valid consent regarding their ad personalization. https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

The GDPR does not explicitly address whether data brokers, who collect consumer data from a variety of sources and create profiles for a number of purposes, may fall under a legitimate interest exception. In 2014, the Federal Trade Commission issued a comprehensive report about the data broker industry ("Data Broker Report").[6] Based on an in-depth study of nine data brokers, it described how data brokers collect personal information about consumers from a wide range of commercial, government, and other public sources and provide it for a variety of purposes, including verifying an individual's identity, marketing products, and detecting fraud. While acknowledging risks to consumers, the Data Broker Report also identified several consumer benefits such as targeted marketing that allows consumers to find more easily goods and services that meet their needs. Importantly, the Report also concluded "consumers benefit from increased and innovative product offerings fueled by increased competition from small businesses that are able to connect with consumers they may not have otherwise been able to reach."

If the data broker model is prohibited outright or made impractical by the GDPR, this may reduce competition in some aspects. Entities that wish to target new customers or create new products but have not collected consumer data themselves may be disadvantaged if they cannot buy or otherwise access such data. Ironically, the GDPR may in this way actually help entrench the position of incumbents who have collected large amounts of consumer data.

The GDPR also grants consumers a number of explicit rights,[7] and, interestingly from the competition perspective, includes a right of data portability. Pursuant to this right, an individual must be able to receive his or her personal data from the data controller, in a structured, commonly used, and machine-readable format and transmit the data to another controller where the processing is based on consent and carried out by automated means. Although this right is clearly related to the GDPR's overall goal of giving people greater control over their data, as other commentators have explained, it also has the additional aspect of possibly enhancing competition by making switching easier and reducing the effects of lock-in.[8]

In sum, the GDPR's overall goal is to give consumers greater control over their data. It may enhance competition to the extent consumers take advantage of the right of data portability and where lock-in and switching costs have been barriers to competition. But, as the FTC concluded in its Data Broker Report, access to consumer data may be an important spur to competition. If the GDPR bars or greatly burdens this access, it may reduce competition.

The FTC Data Broker Report is just one example of the competitive importance of data, including data about or created by consumers. The next section will address how current antitrust law has treated data as an asset and where it has imposed data sharing as an antirust remedy.

III. DATA AS AN ASSET AND DATA SHARING UNDER CURRENT U.S. LAW

Specialized data related to personal information — think real estate records or credit data — have previously been subject to antitrust analysis. In today's online world, however, the debate in competition law circles centers around how to treat data about or created by consumers that is collected through online platforms and used by these entities to target ads, improve current offerings, and create new products. This type of consumer data is often an input for other products and services. For example, Waze (owned by Google) collects and aggregates the location and speed of travel of individual users' phones and uses it to produce dynamic trip directions based on changing traffic conditions. Consumer data is also a commodity asset for advertisers, allowing them to target their ads more precisely, which makes those ads more valuable and thus allows the platforms that hold such data to charge a higher price for that advertising space than other advertising channels.

Antitrust enforcers in the U.S. have experience with competitive issues involving data about or generated by consumers.[9] An example is the 2013 *Bazaarvoice* case, in which the DOJ successfully challenged a merger involving companies that provide software platforms for online ratings and reviews ("R&R") of products created by consumers that manufacturers and retailers host, share, distribute, and display. After a bench trial, the court found a relevant market for R&R platforms and that "syndication, switching costs, intellectual property/know how, and reputation are formidable barriers to new firms entering the market for R&R platforms."[10] The court also found persuasive the fact that both competitors

6 Data Brokers: A Call for Transparency and Accountability, A Report of the Federal Trade Commission (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

7 The GDPR also grants individuals a number of rights, such as access, rectification, and erasure (often called the right to be forgotten).

8 See, e.g. Banda, Carolina, "Enforcing Data Portability in the Context of EU Competition Law and the GDPR," (September 13, 2017). MIPLC Master Thesis Series (2016/17), available at https://ssrn.com/abstract=3203289.

9 See, e.g. Ohlhausen & Okuliar, "Competition, Consumer Protection and the Right [Approach] to Privacy," 80 ALJ 121, 143-46 (listing antitrust cases involving data about or generated by consumers) (2015).

10 See *Bazaarvoice* Memorandum Opinion at p. 133.

referred to each other as duopolists in the R&R market and that Bazaarvoice would have a high market concentration after the acquisition, likely enabling it to charge monopolistic prices.

In *Bazaarvoice*, the court upheld the challenge to the combination of two platforms that used consumer-generated data because of a likely reduction in competition in the market for such platforms, and the DOJ required the defendant to divest the overlapping asset in a settlement. Other merger cases involving specialized data have allowed the merger to occur but required data sharing as a remedy. For example, in a series of mergers involving entities with databases of public real estate records used for title insurance underwriting (called title plants), the FTC has required the merging parties to sell a copy of their title plant.[11]

In another example of data sharing as an antirust remedy (albeit not involving consumer data), in 2015, the DOJ sued to block Cox Automotive's acquisition of Dealertrack. Cox Automotive is the owner of the AutoTrader and Kelley Blue Book brands. As part of its acquisition, Cox sought to purchase Dealertrack's inventory management solution business ("IMS") — a business unit devoted to providing analytics and algorithms to assist car dealers with the management of their vehicle inventory. DealerTrack also held ownership of valuable vehicle information data.

The DOJ was concerned that Cox would not only become an effective monopolist in the IMS market but also would acquire valuable vehicle information data that served as inputs to IMS businesses. With control over that data, Cox could "deny or restrict access" to the data "and thereby unilaterally undermine the competitive viability of Cox's remaining IMS competitors." To allow the deal to go through, the DOJ not only required Cox to divest the IMS portion of Dealertrack's business, it also required Cox to enable the continuing exchange of data and content between the websites it owns and the divested IMS business.

IV. DATA AS AN ESSENTIAL FACILITY

Some would like to take this sharing of data outside the realm of traditional remedies for competitive overlaps in mergers and require data rich companies to provide access to their data assets on the ground that it is simply necessary to compete. In a striking example, last year in Davos, George Soros attacked "giant IT companies" arguing, "[T]he fact that they are near-monopoly distributors makes them public utilities and should subject them to more stringent regulations, aimed at preserving competition, innovation, and fair and open universal access."[12]

In an interesting U.S. case, hiQ — a startup that scrapes data from LinkedIn, analyzes that data, and sells its analytics to businesses for workforce management purposes — sued LinkedIn under California competition law because LinkedIn had sent a cease and desist letter ordering hiQ to stop scraping its data in violation of LinkedIn's User Agreement, citing privacy concerns for LinkedIn users.[13] Notably, hiQ argues that "LinkedIn's conduct violates the 'essential facilities' doctrine, 'which precludes a monopolist or attempted monopolist from denying access to a facility it controls that is essential to its competitors.'"[14] The court granted a preliminary injunction against LinkedIn, finding that there was a reasonable likelihood of success that this claim would prevail on the merits.

The issue of whether companies who accumulate a large amount of consumer data should be required to share it on the basis that it is an essential facility also arose at the European Commission's recent conference on digital policy. In response to a question about whether companies who accumulate large data sets should be forced to share it, Professor Ariel Ezrachi responded that treating big data as an essential facility may be a "worthwhile remedy" to address alleged data monopolization by large tech companies.[15] He cautioned, however, that some information may be private and subject to the GDPR, thus making it different from a typical essential facilities analysis.

---

11 See, Complaint, *Fidelity Nat'l Fin., Inc.*, FTC Dkt. No. C-4425 (Dec. 23, 2013), available at https://www.ftc.gov/system/files/documents/cases/140305fidelitcmpt.pdf; Complaint, *Fidelity Nat'l Fin., Inc.*, FTC Dkt. No. C-4300 (Sept. 16, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/09/100916fidelitycmpt.pdf; Complaint, *Fidelity Nat'l Fin., Inc.*, FTC Dkt. No. C-3929 (Feb. 25, 2000), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/02/fidelitycmp.pdf; Complaint, *Commonwealth Land Title Ins. Co.*, FTC Dkt. No. C-3835 (Nov. 12, 1998), available at http://www.ftc.gov/sites/default/files/documents/cases/1998/11/ftc.gov-9810127cmp.htm; Complaint, *LandAmerica Fin. Grp., Inc.*, FTC Dkt. No. C-3808 (May 27, 1998), available at http://www.ftc.gov/sites/default/files/documents/cases/1998/05/ftc.gov-9710115.cmp_.htm.

12 Buzzfeed.news, "George Soros Just Launched a Scathing Attack on Google and Facebook," 1/25/18.

13 *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

14 *Id.* at 1117.

15 GCR, "Big data is not a typical essential facility, Ezrachi says," 1/17/19.

V. PRIVACY AND COMPETITION: A COMPLICATED RELATIONSHIP

The confluence of privacy and competition law creates numerous dilemmas. Sharing as a competition remedy has traditionally been invoked where data is difficult or expensive to create, raising an entry barrier that keeps out competitors who need access to such data. As discussed above, this has been imposed typically in a merger analysis, where two holders of such a data set want to combine. By contrast, the concern driving privacy law, like the GDPR, is that consumer data has become too widely available, with a perceived loss of consumer control. The remedy adopted for privacy concerns limits collection and restricts sharing of data, except at the consumer's direction. Arguments that consumer data should be treated as an essential facility are hard to square with evidence that data is abundant and available from many sources, as the FTC Data Broker Report showed. The GDPR, or similar laws, are likely to make consumer data harder to obtain and share. Evidence thus far suggests that the GDPR has reduced the collection of data but has also helped entrench some large online companies and hurt smaller players, possibly due to the cost of compliance with the law's complex requirements.[16] Using competition law to force sharing of consumer data as an essential facility, perhaps to mitigate this effect, would undercut the fundamental purpose of the privacy law.

A recent example of this complicated relationship is the German Bundeskartellamt's recent decision that Facebook abused a dominant position as a social network by combining into detailed profiles user data from its own website, its Instagram and Whatsapp services, and from third parties. Though not a data protection agency, the Bundeskartellamt asserted that Facebook violated the GDPR and thus engaged in an exploitative practice that hurt consumers, as well as competitors, who were not able to amass data in the same way. Their proposed remedy is to require Facebook to get consent from users before combining data in this way and to allow consumers to use the services in the same way, even if they do not consent. Whether this blended consumer protection and competition approach will withstand scrutiny or extend outside Germany is unclear, as Facebook has appealed and the head of DG Competition said the decision cannot serve as a template for EU action.[17]

VI. CONCLUSION

Given the raging debate about the role of large tech platforms in our economy and their effects on consumer privacy, competition law and privacy law will continue to interact in complex and sometimes inconsistent ways. In deciding the appropriate relationship between the two, it is important to keep clearly in mind the values that undergird each area of law. Antitrust can take privacy and data, even consumer data, into account to the extent they are tied to a competitive impact, such as when a merger combines specialized data that is not otherwise reasonably available in the market. Invoking it to force data sharing outside these areas is not only unsupported in antitrust law, it may run counter to privacy protections. Privacy law pursues the important goal of helping individuals assert more control over personal data. It can also risk reducing competition, however, and these risks must be taken into account to ensure consumers' interests in both competition and privacy are respected.

16 See, e.g. https://techcrunch.com/2018/10/09/gdpr-has-cut-ad-trackers-in-europe-but-helped-google-study-suggests/.

17 https://www.bloomberg.com/news/articles/2019-02-08/germany-s-facebook-order-will-be-studied-by-eu-vestager-says.

THE BRAZILIAN DATA PROTECTION POLICY AND ITS IMPACTS FOR COMPETITION ENFORCEMENT

BY VINICIUS MARQUES DE CARVALHO & MARCELA MATTIUZZO[1]

1 Vinicius Marques de Carvalho: Professor of Commercial Law at USP, former President of CADE, former Secretary of Economic Law, Yale Greenberg World Fellow and Partner at VMCA. Marcela Mattiuzzo: Master of Laws Candidate at the University of Sao Paulo, Visiting Researcher at Yale Law School, former Chief of Staff at the Office of the President at CADE and Partner at VMCA

I. INTRODUCTION

Four out of ten of the most downloaded antitrust articles of 2018 were about the challenges competition policy faces in the digital economy.[2] While this debate has multiple fronts, discussions about the interface between competition and data protection represent one of the most prominent. In 2016, the French and German competition authorities published a joint paper on the topic, arguing there was much potential data-based anticompetitive conduct to be investigated.[3] In early February the German antitrust authority ruled that Facebook abused of its market power by the hands of "exploitative data collection," in the first case to date to explicitly bridge both fields.[4] In Europe, Commissioner Margrethe Vestager has long defended the need for regulating tech companies and argued data could play a role in constituting market power – especially regarding merger review.[5] In the United States, for its part, the discussions proposed by the so-called Neo-Brandeisian school have caused academics to debate the potential antitrust implications of data collection.[6]

Yet, to discuss antitrust and data protection in Brazil is to navigate uncharted waters. There is no legal device in the country that properly clarifies the interface between the two legal branches. Also, the Brazilian antitrust authority ("CADE") has never directly tackled the issue in any case. Although some individual members of the authority have commented on the topic, there is no official statement about the role data can play in competition policy – which, in turn, does not mean the authority is not interested in the topic.[7] In August 2018, CADE hired a consultant to work together with the Department of Economic Studies to develop a study on the challenges for antitrust in the digital economy. In early February, the authority announced it is recruiting two more consultants to develop works regarding competition and the digital economy.[8]

Also, in late 2018, CADE's Plenary opened an administrative inquiry to investigate potential anticompetitiveness in the payment systems sector regarding data sharing. The case followed a consultation presented by Redecard regarding the legality of a contractual clause that demanded payment acquirers to share some sensitive data with its operations. Despite the matter not being explicitly connected to privacy, when delivering her opinion on the consultation, Commissioner Paula de Azevedo highlighted how the case represented a valuable opportunity to assess the relevance of data from a competition perspective and emphasized that it was relevant for antitrust authorities to be vigilant of the implications of data custody in terms of competition.[9] It is possible to say, therefore, that although CADE seems to be wary of the debates surrounding the topic, the antitrust authority has not voiced an official opinion about it yet.

On the other side, there is uncertainty about how the Brazilian data protection public policy will be structured in the coming years. As this article intends to show, the enforcement of data protection legislation is the focal point which will define what the interplay between competition policy and data protection will look like in the future.

2 Available at https://leconcurrentialiste.com/2019/01/02/the-10-most-downloaded-antitrust-articles-of-2018/.

3 Available at https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.html;jsessionid=94562779C7216ECF430D4C112D1E4306.1_cid371?nn=3591568.

4 The full decision is not yet available but the Bundeskartellamt published a FAQ and a press release about the case, both of which are available in English at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

5 For example, one of her latest announcements summarizes these opinions presented https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/protecting-consumers-digital-world_en.

6 Wu, Tim. The Curse of Bigness: *Antitrust in the New Gilded Age*. Columbia Global Reports, 2018.

7 For example, former-Commissioner Cristiane Alkmin Junqueira Schmidt has written short article defending the consumer welfare standard should encompass considerations other than price, such as data privacy. Available in Portuguese at https://www.jota.info/opiniao-e-analise/colunas/coluna-da-cristiane-alkmin/hipster-antitrust-poder-de-mercado-e-bem-estar-do-consumidor-na-era-da-informacao-28122018.

8 While one of the researchers will carry out research about this interface in BRICS' countries, the other shall conduct a more general international benchmarking about competition and digital economy as well as organize an international seminar and workshop about it. Information about these recruitment processes can be found at http://www.cade.gov.br/acesso-a-informacao/concursos-e-selecoes.

9 Consultations n°s 08700.004009/2018-41, 08700.004010/2018-76, 08700.004011/2018-11 e 08700.004012/2018-65, all jointly presented by Redecard.

II. THE NEW DATA PROTECTION LEGISLATION IN BRAZIL

Brazil did not have a General Data Protection Act ("GDPA") until August 2018. The LGPD, as it is known by its Portuguese acronym, creates a new legal framework for the treatment of personal data in Brazil, both online and offline, in the private and public sectors – complementing and to some extent substituting the former diffuse sectoral-based regulatory framework. The topic was the subject of a broad discussion in the Legislative branch, with different bills being debated in the two houses of Congress.

After approval by the Congress, bills are subject to presidential approval or veto. On August 14, former President Michel Temer vetoed some provisions of the new law, including the creation of the national data protection authority, arguing that the inclusion of the agency was legally flawed.[10] The expectation was for the issue to soon be resolved, with the creation of the authority through a separate instrument. Although the LGPD is only set to come into effect in 2020, the veto raised concerns because the authority supported the whole data protection regulatory system and would hold an important role in both structuring the public policy and making sure it works accordingly.

Since August, interest groups, including non-governmental organizations, academics, and representatives from the private sector, pressed the Government to enact the complementary LGPD legislation. In addition to the reasons already mentioned, the topic gained urgency as a result of the Brazilian presidential transition in 2019 – Temer would step down in December 2018 and a new government would take office starting January 1, an administration that provided little clarity during the presidential race on how it would tackle the matter and what its commitment to the data protection legislation would be.

On December 28, the Executive Order was published, creating the National Data Protection Authority ("ANPD").[11]

The structure of the ANPD is different from that set forth in the original bill: instead of adopting the autarchy-model, which is the structure of most regulatory agencies in the country, the ANPD was envisioned as a federal public administration entity, subject to the control of the Office of the President. In other words, instead of being autonomous, the authority will be closely connected to the government, which raises concerns regarding the path to be followed by the data protection public policy in Brazil, especially regarding the applicability of the LGPD to the public sector.[12]

Experts discussing the implementation of the GDPA had already pointed towards the importance of centralized enforcement, which would ensure a single forum for the debate of the regulations with stakeholders, secure technical soundness of the decisions, and facilitate coordination with other agencies and public policies that will be affected by the new rules – e.g. the GDPA's specific provisions addressing data related to healthcare, which naturally implicates the National Health Agency.

III. DATA PROTECTION AND COMPETITION – THE INTERPLAY BETWEEN PUBLIC POLICIES

Regarding competition, this development is crucial. As mentioned, CADE has so far addressed data-related matters in a rather timid manner, carefully weighing when and if the allegations bear significance for antitrust. It has, however, suffered pressure from some stakeholders who believe it should be more active, embrace more data concerns, and use the investigations currently underway to send a message to the private sector. Perhaps the most meaningful example is the study developed in 2018 by Intervozes.

Intervozes is a civil society organization focused on promoting the right to communication in Brazil. In May 2018 it launched a study on "Digital Monopolies: Concentration and Diversity on the Internet" with the far-reaching aim of identifying the degrees of concentration and diversity on the Brazilian Internet, looking specifically at apps and content providers.[13] Although suffering from conceptual inaccuracies, the study encourages antitrust scrutiny to face the "perils" associated with the digital economy. When launching the study, the organization highlighted

10 Although the bill that later came to be the LGPD was proposed by the Executive, the inclusion of the data protection authority was carried out by of a member of the Legislative. The Office of the President alleged this constituted a violation of Articles 61, § 1º, II, 'e' and 37, XIX of the Brazilian Constitution.

11 Executive Orders are legislative acts through which the President can enact legislation that comes into force immediately, without the approval of the National Congress. Before becoming permanent, however, the orders must be approved by the National Congress in no more than 120 days. In this sense, there is still some uncertainty when it comes to the actual creation of the authority, for Congress may still impose changes on the system currently in place.

12 The LGPD applies both to private and public sectors, though regulations differ in what they require entities to treat personal data.

13 The English version of the study is available at http://monopoliosdigitais.com.br/site/wp-content/uploads/2018/11/Monopolios_Digitais_INGL%C3%8AS.pdf.

potential privacy violations arising from companies placed in the data-driven economy.[14]

The establishment of a data protection authority ("DPA") might to some extent minimize the pressure exercised by stakeholders upon CADE, for data related issues would gain a specific forum and the tendency would be for interested parties to address their concerns to this new agency. Moreover, the creation of a DPA would go a long way towards organizing and clarifying the role of data protection when it comes to competition policy. If CADE follows the same line of dialogue set forth with other agencies, the approach would be complementary and the agencies would tend to work together; CADE would also be inclined to respect the specialized agency's takes on data protection, for it traditionally understands the regulatory actor to be better suited to decide the direction of the public policies under their command.

Some may argue that in light of the recent Bundeskartellamt decision condemning Facebook's data collection strategy these observations lose weight. The German authority decided that Facebook's terms and conditions were exploitative and amounted to abuse of market power, and explicitly recurred to data protection legislation to do so.[15] Moreover, although personnel at the authority had previously stated that the case would have never been started had the data protection authorities done their job, the antitrust enforcer emphasized that:

> Social networks are data-driven products. Where access to the personal data of users is essential for the market position of a company, the question of how that company handles the personal data of its users is not only relevant for data protection authorities, but also for competition authorities. […] Monitoring the data processing activities of dominant companies is therefore an essential task of a competition authority, which cannot be fulfilled by data protection officers. In cases of market dominance a competition authority must take into account data protection principles, in particular in the assessment of whether terms and conditions for the processing of data are appropriate. In this respect there is an interface between competition law and data protection law.[16]

Again, the decision of the authority has not yet been published, and hopefully it will make this statement both clearer and more robust, but we do not believe it weakens our claim that Brazil would benefit from a strong DPA and that this would help organize enforcement.

Establishing a model for interaction between policies does not mean CADE would be passive in cases regarding data, but merely that the jurisdiction of each authority would be clearer and therefore less undue pressure for the competition authority to take action that falls outside its mandate would exist. The Brazilian antitrust agency is of the understanding that there is no antitrust immunity in regulated sectors and that the agencies and CADE have concurrent jurisdiction (the possible exemption is the financial sector).[17] In those occasions, CADE usually restricts its action to competition matters while the regulatory agency remains responsible for the sector-specific affairs.

In the recent merger review of the *AT&T-Time Warner* deal, for example, CADE's Tribunal ruled that the antitrust agency should not block the acquisition under a provision of the Cable TV law which prohibits vertical integration between a provider of telecommunications services (such as AT&T) and a television programmer (such as Time Warner).[18] In their analysis, the Commissioners were clear that CADE should limit itself to a standard antitrust approach, approve the merger, and leave the regulatory aspects to the Telecommunications Agency, even though they expressly recognized that under the Cable TV Regulation the transaction should be blocked, given that the proposed structure of the future

14 The study also suggests potential anti-competitive practices conducted by the so-called digital monopolies. For example, regarding Google, it mentions how the prioritization of ownership services in search results could represent an antitrust issue.

15 As mentioned, the decision itself is not yet available, but the Bundeskartellamt has already said that "If a dominant company makes the use of its service conditional upon users granting the company extensive permission to process their personal data, this can be taken up by the competition authorities as a case of 'exploitative business terms'. According to the case-law of the German Federal Court of Justice, civil law principles can also be applied to determine whether business terms are exploitative. Often such principles stem from the legislation on unfair contract terms or the German Constitution. This applies to any legal principle that aims to protect a contracting party in an imbalanced negotiation position. Following this approach, the Bundeskartellamt applied data protection principles in its assessment of Facebook's terms and conditions. […] On the basis of data protection principles, in particular under the General Data Protection Regulation (GDPR) applicable since May 2018, the review of the data processing policies showed that Facebook has no effective justification for collecting data from other company-owned services and Facebook Business Tools or for assigning these data to the Facebook user accounts."

16 Available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5.

17 The issue was first addressed on the Administrative Proceeding 20/1992, in which public transport companies from Belo Horizonte were accused of cartel formation and declared in their defenses that CADE could not fine them since there was already an agency overseeing their activities. By that time, CADE understood that the only situation in which this allegation could be valid was under the State Action Doctrine, as developed in the American antitrust case law, and that the existence of a regulation or a regulatory agency did not prevent CADE from acting to put an end to anticompetitive behavior in any way. Since then, a number of cases, especially in conduct control, reinforced this understanding.

18 The deal was reviewed under the number 08700.001390/2017-14 and approved in October 17, 2017. The Telecommunications Agency, nonetheless, has not reached a decision so far.

company would clearly violate Article 5 of the sectorial legislation.[19] The merger was therefore approved by CADE, but still awaits the approval of the Telecommunications Agency, which shall decide on the matter of Article 5.

In fact, this tendency to separate the spheres of influence and maintain distinct competition and regulatory mandates dates back to CADE's early years and has been reaffirmed in several opportunities. One example is the Administrative Proceeding in which two gas companies were accused of abusive pricing for raising their prices according to the determination of the competent agency – which at that time was responsible for setting prices.[20] In CADE's view, the agency was pursuing a clear and legitimate goal and the companies were simply following its determinations. Since there was no option other than to follow the determined price increases, CADE ruled that the companies could not be fined and that the regulation should be upheld.

Moreover, CADE has signed cooperation agreements with several federal agencies to ensure that both it and its regulatory counterparts can maintain their separate jurisdictions while collaborating to preserve autonomy and ensure the most appropriate decisions, considering regulatory and competitive aspects. Some examples are the agreements signed with the Brazilian Central Bank, the National Agency of Electric Energy, and the National Petroleum Agency; all of which are intended to better address competitive issues that relate to regulatory provisions.

In that light, it is certain that the implementation of a DPA is central in understanding how antitrust and data protection will interact over the next years, considering CADE's own comprehension of its jurisdiction when it comes to regulated matters in which other actors play an active role. Some provisions of the Executive Order reinforce this conclusion. Article 55-J, Paragraphs 2 and 3, as well as Article 55-K determine that the ANPD is the sole entity responsible for applying the sanctions set forth in the GDPA, that it shall coordinate enforcement with other public entities responsible for regulating specific economic sectors, and that its authority will always prevail in data protection matters when faced with other institutions.[21]

However, the confirmation of this prediction largely depends on two factors: first, the success of the data protection public policy – here meaning precisely the effective establishment of a robust authority able to coherently apply the new legislation. Second, the DPA's willingness to engage in dialogue with other public institutions to coordinate enforcement. Not only CADE, but also the ANPD would have to be committed to reaching a balance and to working together to set the boundaries of data protection and competition, deciding where cooperation would be profitable, where enforcement by the DPA would suffice, and where antitrust would be a more appropriate tool. The success of this "alliance" is highly dependent on the first factor: it is natural for the competition authority to be more deferential to an agency that actively embraces its objectives and puts forward a coherent policy. In that sense, the lack of autonomy for the DPA, a loose application of the GDPA, and a lack of confidence of the authority on the part of stakeholders all could work against the fulfillment of our hypothesis and impair the establishment of a dynamic similar to the one already set between CADE and other agencies.

Little certainty on how those issues will be addressed exists. The fact that a new administration just took office, and that the ANPD was created by the precarious Executive Order method, contributes to the unpredictability of what is to come. What remains, however, is the need to address the matter and the understanding that data-related issues are bound to arise with ever more prominence in the future.

19 Article 5 of the Law n° 12.485/2011 states that content providers shall not be vertically integrated with telecommunications service providers. In this case, AT&T functions as a telecommunications provider in Brazil, represented by SKY, and Time Warner delivers content in the country. To illustrate the echo of the regulatory norm in CADE's analysis, it is worth mentioning that Ms. Cristiane Alkmin's opinion expressly declared that under a regulatory approach the deal could not be approved at all.

20 See Administrative Proceeding 08012.006207/1998-48 involving Riogás S/A and Companhia Estadual de Gás do Rio de Janeiro – CEG.

21 Article 55-J, § 2: The ANPD, the agencies and public entities responsible for the regulation of specific sectors of economic and governmental activity shall coordinate its operation, in its corresponding sphere of activity, with the aim of ensuring the enforcement of its responsibilities with the maximum efficiency and of promoting the adequate functioning of regulated sectors, according to specific legislation, and personal data treatment, as provided in this Law. § 3: The ANPD shall keep permanent communication forum, including through technical cooperation agreements, with agencies and public entities responsible for the regulation of specific sectors of economic and governmental activities, with the aim of facilitating ANPD's regulatory and enforcement competences. Article 55-K: The application of the sanctions provided by this Law is exclusive to the ANPD, whose other competences should prevail over other agencies or public entities when focused on personal data protection. Sole paragraph: ANPD shall articulate its activities with the National System of Consumer Protection associated with the Ministry of Justice and other agencies and public entities with normative and disciplinary competences related to the theme of personal data protection and shall be the central agency responsible for the interpretation of this Law and provision of norms and guidelines for its implementation.

DATA PROTECTION AND ANTITRUST: NEW TYPES OF ABUSE CASES? AN ECONOMIST'S VIEW IN LIGHT OF THE GERMAN *FACEBOOK* DECISION

BY JUSTUS HAUCAP[1]

1 Professor of Economics at the University of Düsseldorf, Director of Düsseldorf Institute for Competition Economics ("DICE"). Disclaimer: Two years ago, the author wrote a short expertise on the role of data in social networks on behalf of Facebook. He has neither been active for Facebook since then nor has he discussed any details of the German *Facebook* case with either Facebook or any of its representatives since then. The author is also a member of the German Federal Cartel Office's economics expert working group on competition economics.

I. INTRODUCTION

Many services on the Internet are seemingly offered for free, people do not have to pay for them, at least not with money. Instead, it is regularly argued, people are paying with their (personal) data. If people are not paying with money, but with data, however, the question emerges how antitrust laws can be applied to these particular markets.

How difficult it is to define markets in the absence of monetary prices has been discussed in the literature at length by now. Less attention has been given to the question of whether and, if so, how data protection and privacy concerns should be part of antitrust enforcement. Three different issues can be distinguished in this context. First, there is the question of what kinds of behavior (if any) may be considered exploitative abuses by dominant firms in markets where customers are not paying with money, but – as it may seem – with data. This is, by and large, at the heart of the Federal Cartel Office's *Facebook* case in Germany, the decision of which has long been eagerly awaited and was finally announced on February 7, 2019, even though the text of the decision has not been published yet.[2] Second, a question emerges whether denying competitors access to certain types of data may be considered an obstructive abuse or anticompetitive exclusionary behavior that unduly impedes effective competition. And third, a question arises whether the effects that arise from the acquisition and combination of data sets should be subject to distinct consideration in merger analysis.

II. DATA USAGE BY DOMINANT FIRMS AS EXPLOITATIVE ABUSE?

Let us start with analyzing the first question, which is also decisive for the German *Facebook* case: What kind of behavior constitutes an exploitative abuse in markets where people do not pay with money for the services they use? In principle, the underlying idea pursued by the Federal Cartel Office appears to be quite simple: Excessive pricing by dominant firms is unlawful in many countries, for example under Article 102 of the Treaty of the Functioning of the European Union. Hence, once users are "paying with data," a dominant Internet firm's use of customer data may also be considered excessive. Put differently, if a firm asks its customers for "too much" data and is "too intrusive" with respect to users' privacy in return for its services, this may be considered an exploitative abuse of market power analogous to excessive pricing. However, as is often the case with simple ideas, things become more complicated at second sight.

First of all, data is not like money. Providing personal data to an online service does not reduce the user's ability to provide the same data to another service or multiple other services. Hence, while in public discussions data is often portrayed as "the new oil" or as a means of payment, these analogies are highly misleading. Oil is an exhaustible resource and a private good that cannot be used either in parallel or sequentially by different users, while data can be used multiple times and at the same time by many services. Similarly, the idea that data is a means of payment is misleading, as – unlike money – the same data can be shared with multiple users multiple times. Even if a user "pays" with data for a particular service, the user's amount of data available to him or her is not reduced. His or her wealth in terms of available data is not affected. In that way, "paying with data" is quite unlike paying a monetary "price." Hence, it is conceptually much more difficult to construct an exploitative abuse case, as users are not left with less data than they had before. This is a fundamental difference to excessive pricing cases where customers are left with less money/wealth once they have been exploited. If a resource can be used infinitely often without incurring any additional cost, however, it is not possible to exploit that resource or its holder.

However, while users may not be exploited with respect to their data, their privacy may be reduced, possibly unduly so. In fact, this view is closer to the FCO's theory of harm. According to the FCO, Facebook's behavior is exploitative *vis-à-vis* its users because users are losing control about how their data is used.[3] Still, for a reduction in personal privacy (and excessive data requirements) to be similar to a reduction in personal wealth (and excessive pricing), people actually need to care about privacy. At this point, it is noteworthy that, quite generally, many people willingly consent to other parties' using their personal data if this increases the quality of the services they are interested in. While it is true that many people, when asked in public, maintain that they are concerned about how their personal data is used and that they are rather protective about how their data is used, these stated preferences are not revealed in their actual behavior. Put differently, a substantial body of empirical and experimental evidence has consistently found over and over again that even a vast majority of individuals who maintain to be heavily concerned about privacy are willing to share personal data in return for rather small forms of compensation or improved services.[4] This finding has been

2 The Federal Cartel Office published a summary of the case on February 15, 2019, available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf.

3 See Bundeskartellamt (2019), Facebook FAQ's, online at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf.

4 See, e.g. Acquisti, A., C. R. Taylor & L. Wagman (2016), "The Economics of Privacy," *Journal of Economic Literature* 54, pp. 442-492; or Benndorf, V. & H.-T. Normann (2018), "The Willingness to Sell Personal Data," *Scandinavian Journal of Economics* 120, pp. 1260-1278.

coined the "privacy paradox."[5]As, however, preferences revealed through actual behavior are typically taken to better reflect individuals' true preferences than surveys, it appears that many people willingly share their data in order to obtain better services. Given these findings, it is difficult to conceive how users can be exploited if they willingly share their data. Overall, however, we may need to broadly distinguish between two types of potential users: Those who really care about their personal data and their privacy and those who do not, but happily share their data.

If users of a particular Internet service do *not* mind if their personal data is used by the service provider, this means that they do not receive disutility from sharing personal data and having data sets combined. In these cases, collecting and combining data from these users can hardly be an exploitative abuse, as consumers cannot be exploited if they do not mind providing the data that is collected. Put differently, there can hardly be any harm inflicted onto these users if they do not receive any disutility from having their data combined. On the contrary, as combining data typically facilitates the development of better matching technologies to rank offerings, news, and other information to match user interests, the prohibition to do so would lead to a deterioration of the services offered (as the matching technology would deteriorate).

In addition, as a rule of thumb, it appears safe to assume that users at least weakly prefer advertising that matches their interests over advertising that does not coincide with their interests ("spam" at the extreme). Hence, better matching users and advertisers should, if at all, increase users' utility from using a particular service and clearly increase the benefits that accrue to both users and advertisers. Put differently, the quality of a platform's matching technology does not only affect advertisers, but also tends to benefit users. Generally speaking, the quality of any matching technology depends, in part, on the amount, but also on the quality of information available to be used by the technology, along with a host of other factors. Hence, the benefit received from a particular service, for both users and advertisers, is a positive function of the amount and quality of information available to be used to match users with content that may interest them, both organic and advertising. In this context, access to and use of different sources of data (e.g. off-Facebook data and on-Facebook data, which is at the heart of the German *Facebook* case) allows for better matching than the use of just one source.

The case is different, of course, 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. But even for these cases, it is not clear that antitrust laws are best for dealing with these valid concerns. Virtually all jurisdictions have specific laws regarding data protection and privacy that typically apply to all firms and transactions regardless of market power. It is obvious that firms with market power have to adhere to these standards in the same way as firms without (substantial) market power. It is unclear though, at least from an economic perspective, why a breach of privacy and data protection laws would also, in addition, constitute a breach of antitrust laws. Put differently, since a breach of data and privacy laws by firms without market power cannot be an antitrust abuse, why would the same behavior by dominant firms constitute a breach of antitrust laws? The question appears to be whether antitrust laws should hold dominant firms to stricter data protection and privacy standards than competing firms without market power are held to by general data protection and privacy laws. From a competition policy perspective, it is difficult to conceive of good reasons for such a policy.

In fact, hypothetically requiring dominant firms to use or combine less data or only data from certain sources and to offer higher privacy standards than what is legally required from competing firms without market power would be equivalent to requiring dominant firms by law to offer – from the perspective of those users who heavily care about privacy - superior products than rivals – a requirement, which could – in the extreme case – even foreclose the market, as data-sensitive consumers would basically be guaranteed higher privacy standards with dominant firms.

At the same time, a dominant firm in the "user market" may become less competitive in advertising markets *vis-à-vis* competitors form other "user markets." And, finally, as data is used to develop and offer better services at least in the eyes of those consumers who do not mind sharing their data, preventing firms from collecting, combining, and using data beyond what is regulated by privacy and data protection laws is equivalent to requiring the firm to be less innovative and to offer inferior services – both of which would harm competition.

Still, a situation may emerge where dominant firms can "force" their users to consent to the use and combination of levels of data which non-dominant firms may not be able to obtain from their customers. In fact, this appears to be the FCO's key objection regarding Facebook. The dominant firm's access to more data is likely to help the firm to improve and tailor its services to user preferences and also to increase advertising efficiency. Here a difficult trade-off emerges, as requiring dominant firms to collect and to combine less data will typically also imply a deterioration of service quality and advertising efficiency, and thereby, a softening of competition. While some consumers may prefer higher privacy standards even if this reduces service quality, other consumers may happily share their data in exchange for better-tailored services. In the past, therefore, the idea has been brought forward that dominant firms should be forced to offer consumers two forms of "payment": Consumers

5 See Norberg P. A., D. R. Horne & D. A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* 41, pp. 100-126.

should be free to either pay with their data or with their money. There are several problems with this suggestion, however. First, it is unclear what the competitive price in monetary terms should be, given that it has not emerged in the market for most services that are under consideration. Second, firms use the information not only to improve advertising efficiency, but also the product itself. Hence, the more consumers chose to pay with money, the lower the service's quality will inherently become, as data is a critical input to improve the services. While users who do not provide data may individually receive lower service quality levels, the overall quality of a matching algorithm will also deteriorate as less information on users' preferences and behavior is available.

Consider the case of social networks as an example: Typically, social network users are fairly heterogeneous in their motives as to why they use social networks. While some users tend to be more active and send out and share personal information, comment on other users' activities, and engage in discussions, other users tend to be more passive and, instead, receive and consume information provided by other users (i.e. they may "follow" others' activities rather than using social networks as a "broadcasting" medium). Of course, many people tend to engage in both information sharing and consuming activities at various times, but for analytical purposes it is helpful to distinguish between sharing and consuming activities, keeping in mind that users are "senders" at one point in time and "receivers" at others. "Senders" tend to benefit if they are able to reach interested "receivers," while "receivers" benefit from relevant information broadcasted by "senders," as this increases the likelihood of receiving interesting or engaging content.

It is important, though, to note that the user benefits of sending and receiving information do not simply increase with the amount of information received and the number of potential receivers addressed. If "senders" share information with many people, but most "receivers" do not find the information useful or interesting, the "sender" may not really benefit from sending out the information- just as commercial advertisers do not benefit if they target the wrong audience. Similarly, "receivers" do not benefit from an increase in the amount of information if they find the information offered uninteresting and useless. Quite in contrast, receiving more information of little interest (which may be considered "spam") will even decrease "receivers'" utility, as they will find it more difficult to sort out the more interesting updates from the less interesting ones, especially if such an increase in information leads to information overload. Hence, both "senders" and "receivers" tend to benefit from better matching technology. "Receivers" benefit the better the information highlighted to them is. Similarly, when users share information they benefit if the information they share primarily reaches people who are interested in that particular information. If, in contrast, the information shared is received by users who do not find that information useful or neglect it, the "sender" receives less benefit from sharing his information, assuming that people share information with the purpose of reaching an audience who finds the information useful or interesting. If the matching mechanism for information shared and information received is improved, user benefits increase. Hence, better matching any type of content with user interests increases the utility of the social network for both "senders" and "receivers."

Finally, forthcoming empirical evidence even suggests that larger firms often tend to offer more privacy than small ones.[6] Hence, it becomes unclear which privacy level would prevail at the competitive level – the standard hypothetical counterfactual for antitrust abuse cases – and which level would be considered abusive.

In its *Facebook* case, the German competition authority is particularly concerned about Facebook's practice of collecting data from outside the Facebook universe. In fact, Facebook collects data about its users and even non-users via apps such as WhatsApp and Instagram that are owned by Facebook and also via third-party apps and webpages that use Facebook interfaces, for example, in the form of Facebook-like-buttons that are integrated in many webpages. However, while these practices may possibly violate privacy and data protection laws, it is still unclear how they relate to Facebook's market power, and whether and how consumers are exploited beyond the harm possibly inflicted by potentially violating privacy and data protection laws.

In sum, Internet users and advertisers both tend to benefit from the use and combination of data, as the usage and combination of different data sources facilitates the improvement of matching algorithms to offer services, rank information, and provide news for users. The case is different, however, if some users receive direct disutility from their data being used. In these cases, however, data protection and privacy laws appear to be the proper statutes to regulate firms' behavior. It is not clear from an economic perspective why firms with market power should be held to stricter privacy standards than firms without market power, as such a practice may distort, rather than protect, competition. Moreover, it is at best unclear whether small firms adhere to stricter privacy standards than large firms. If, however, the opposite is true, the question emerges what the appropriate benchmark for abuse cases should be. Requiring dominant firms to behave more like competitive firms would be rather absurd if small firms without market power violate privacy standards more often than larger firms.

6 Sabatino, L. & G. Sapi (2019), "Online Privacy and Market Structure: An Empirical Analysis," DICE Discussion Paper No. 308, available online at https://ideas.repec.org/p/zbw/dicedp/308.html.

The FCO also suggests that users may not always be aware of what kind of data is collected and how this data is used due to a lack of transparency. This, however, appears to be by and large a problem of asymmetric information which is not necessarily related to market power. Put differently, information asymmetries are often also exploited in competitive markets with small firms, as George Akerlof already suggested in his famous used car dealer example.

Also, any analogy with data as a form of money or payment is misleading, as monetary resources cannot be used multiple times. Finally, empirical evidence suggests that (many) people do not feel exploited when their data is used. Quite in contrast, a fair number of people tends to willingly share data in order to obtain benefits such as improved services. This is probably especially true for social networks where many people "broadcast" personal information about their activities. Against this background, it is conceptually rather difficult to establish sound evidence that collecting and combining users' data constitutes an exploitative abuse of market power, especially when considering the fact that small networks and Internet service providers without market power also engage in comparable practices.

III. DATA USAGE BY DOMINANT FIRMS AND OBSTRUCTIVE ABUSE OF MARKET POWER?

At least from a conceptual point of view, situations in which dominant firms deny third-party access to certain types of data may be more easily conceived as an (obstructive) abuse of market power. Put differently, situations may emerge in which – due to network effects and economies of scale – a dominant firm has collected such an amount of data that competitors may not be able to duplicate the same or a functionally equivalent set of data and, therefore, suffer from a substantial competitive disadvantage. In the extreme case, certain data may be considered an essential facility to which competitors need access, unless there are valid justifications for not grating access- such as, for example, privacy and data protection laws. Nevertheless, depending on the particular circumstances, sometimes even anonymized or pseudonymized data may be sufficient to facilitate competition. For the Google search engine, for example, some authors have argued that granting third party-access to historical search and click data would solve most of the competition concerns.[7]

From an economic viewpoint, there are good reasons why, in principle, third-party data access should be granted more easily than in the case of classical essential facilities such as physical networks or other infrastructure. First, classical infrastructure is often rival in usage. Once a competitor has taken over the incumbent's local loop, the incumbent cannot use the relevant lines itself anymore. Similarly, if a certain slot for a railway track is used by a new entrant, the same slot cannot used by the incumbent any longer. In contrast, even with third-party access to data, the incumbent can still use the data itself. Hence, access to assets or facilities that are not rival in usage should be granted more easily. Second, physical infrastructure typically requires significant investment and maintenance expenditures. Therefore, antitrust law and regulation have established rather high legal thresholds for third-party access in order to preserve the investment and maintenance incentives. In contrast, while data collection and maintenance can also require significant investment, this is not always the case. Instead, data is often generated and collected as a by-product without significant investment efforts by the collector. If, then, incumbents can collect data without significant investment, the threshold for third-party access should be systematically lower than for traditional essential facilities.

Overall, the fact that (a) data is typically non-rival in usage and (b) data is at least sometimes collected by incumbents without significant investment together suggest that the threshold for third-party access should, in principle, by systematically lower than for classical infrastructures. Data protection and privacy laws play a role in these cases; however, they may also provide valid justifications for why third-party access to data may not be granted in some cases.

In the FCO's prominent *Facebook* investigation mentioned above, access to data or data sharing has not played any role. However, the FCO's second theory of harm circles around the effects that Facebook's data collection efforts have on competitors, more precisely the effects of Facebook's data collection activities in advertising markets. Interestingly enough, the FCO has found Facebook to be "the dominant supplier of advertising space in social networks," suggesting that "advertising in social networks" is a separate antitrust market in its own, separate from other online advertising markets. It remains to be seen what evidence there is to suggest that Google (which does no longer operate social networks, as YouTube does not appear to be part of the relevant market in the FCO's eyes) and Facebook do not compete for online advertising in the same market. Be it as it may, the FCO's theory of harm with respect to advertising markets mainly consists in Facebook being able to collect and combine so much data that it can easily outcompete its rivals, as it can better target advertising – by and large an efficiency offense, which may even benefit users if they prefer more targeted advertising over advertising that is less related to user preferences.

7 Argenton, C. & J. Prüfer (2012), "Search Engine Competition with Network Externalities," *Journal of Competition Law and Economics* 8 (1), pp. 73-105.

IV. DATA PROTECTION AND MERGER POLICY

Finally, new challenges emerge for merger policy, as the potential combination of data sets may give rise to new competition concerns not only in horizontal and vertical, but also in conglomerate mergers. In many instances, however, the combination of data sets will give rise to new efficiencies as long as the combination of data sets either increases the productivity of production and/or distribution activities, or facilitates the supply of tailor-made products or services. Moreover, data protection and privacy laws obviously also apply to merged entities. As long as data protection and privacy laws regulate firms' behavior with respect to their usage of data, there does not appear to be an additional role for merger policy with respect to data protection.

In the context of the FCO's *Facebook* case, an interesting observation is that the FCO has chosen a rather narrow market definition for social networks, explicitly excluding WhatsApp from that market. While this is certainly helpful for the FCO in bringing its abusing case, it also contrasts with thinking by the European Commission's chief competition economist Tommaso Valletti whether we should not define markets for attention (which is truly a scarce resource). From a merger policy perspective, defining markets for attention is, of course, attractive for competition authorities as it allows them to tackle Facebook's acquisitions of WhatsApp and Instagram more easily. Abuse cases, however, become more difficult under such a market definition, as it would be much less clear whether Facebook would be dominant in a market for attention. In order to apply competition law in a consistent fashion, markets need to be defined in a consistent way, either as markets for attention or more narrowly, independent from whether mergers or potentially abusive behavior is investigated.

V. CONCLUSION

For many Internet services, users do not pay with money, but rather pay with their (limited) attention. While users are sometimes said to pay with their data for these services, this analogy is rather misleading, as users' data is, unlike money, not limited – quite in contrast to users' attention. As data is, in principle, not limited, it is much more difficult to conceive what use of data would constitute an exploitative abuse of market power – the issue which is at heart of the German antitrust case into Facebook's data combination practices. Moreover, since data is typically used to improve the respective services, it should be much more difficult to provide sufficient evidence that the usage of data constitutes an exploitative abuse of market power that harms consumers. In addition, as smaller networks and service providers without market power do not appear to systematically adhere to stricter privacy and data protection standards, it becomes difficult to envisage what the appropriate counterfactual should be that dominant firms need to adhere to. A hypothetical requirement for dominant firms to adhere to stricter privacy standards would, also, very likely distort rather than safeguard competition. As a consequence, portraying data usage as analogous to excessive pricing is fraught with difficulties.

In contrast, it is easier to conceive that not granting third-party access to data may be an obstructive abuse of market power. Moreover, as data is – in contrast to many other facilities – non-rival in use and, at least in some cases, not associated with significant investment expenditure, the legal threshold for third-party access should generally be lower than for classical essential facilities, such as physical network infrastructures.

THE GERMAN *FACEBOOK* CASE – TOWARDS AN INCREASING SYMBIOSIS BETWEEN COMPETITION AND DATA PROTECTION LAWS?

BY DR. JÖRG HLADJK, PHILIPP WERNER & LUCIA STOICAN[1]

1 Dr. Jörg Hladjk, Partner, Jones Day, Cybersecurity, Privacy & Data Protection Practice, Brussels. Philipp Werner, Partner, Jones Day, Antitrust & Competition Practice, Brussels. Lucia Stoican, Associate, Jones Day, Antitrust & Competition Practice, Brussels. The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of the law firm with which they are associated.

I. INTRODUCTION

The rise of multi-sided online platforms like Amazon and Facebook, that collect, process, and monetize huge amounts of users' data for profiling and targeted advertising has created controversial issues under both competition and data protection laws. This has especially been accentuated in Europe due to the entry into force of the GDPR in May 2018[2] and due to the recent spotlight on tech companies – coming from both competition and data protection enforcers.[3]

Competition authorities around Europe have expressed concerns that – while data becomes "the oil of the 21st century" – a handful of companies are gaining control over it and "real competition" for the market becomes virtually impossible. The identity crisis of the rule of law system in the tech area is evident in a recent statement of EU Commissioner Margarethe Vestager: "we do not know if we should just reinterpret the rules we have already or to what degree we should add new rules."[4]

The struggles of an obsolete rule of law system to deal with high tech and big data are also reflected in recent decisions. While in the *Facebook/Whatsapp* merger, the European Commission summarily noted that "privacy-related concerns flowing from the increased concentration of data within the control of one company (…) do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules,"[5] in the subsequent *Microsoft/Linkedin* case the Commission nuanced its position and clarified that "privacy-related concerns (…) can be taken into account in a competition assessment to the extent that consumers see it as a significant factor of quality."[6]

Recently, one of the world's most respected antitrust authorities – the German Federal Cartel Office ("FCO") – was also called to examine these issues in the context of proceedings launched in 2016 against Facebook for an alleged abuse of dominance. More specifically, in its preliminary legal assessment,[7] the FCO considered that Facebook is abusing its dominant position in the market for social networks through the imposition of "misleading" data protection policies to its users. Interestingly enough, the FCO seems to be more forward looking than the European Commission, underlining that **monitoring the data processing activities** of dominant companies is an **essential task of the competition authority**, which cannot be fulfilled by a data protection authority.[8] In its assessment of whether the company's terms and conditions on data processing are unfair, the competition authority does, however, take account of the legal principles of data protection laws by noting that "for this purpose, the Bundeskartellamt works closely with data protection authorities."[9]

The outcome of the German *Facebook* proceedings is of much interest for the development of both EU competition and data protection laws.[10] It will most likely set a precedent, since it is the first time that an infringement of data protection rules will be examined by a competition enforcer under abuse of dominance rules. Could this case therefore pave the way to a convergence between competition and data protection rules? Could this convergence result in a data sharing obligation imposed by competition enforcers on companies that are abusing their dominant

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

3 Europe, in particular, has focused significant attention on competition, big data, and regulation of digital platforms. Recent landmark cases in the EU include the Commission's €110 million fine against Facebook for having provided misleading information about the way the users' private data would be handled post-merger with WhatsApp, and Germany's investigation into Facebook's practice of forcing customers to agree to unfair terms about the way the company uses their data; See case M.8228, *Facebook/WhatsApp*, [2017] OJ C286/06; Commission decision of January 24, 2018, *Qualcomm*, case AT.40220; Judgment of October 6, 2015, *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650; Judgment of the Regional Court of Berlin of January 16, 2018, docket no. 16 O 341/15; Italian Competition Authority, Press release of November 29, 2018, Facebook, http://www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-degli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Facebook, accessed on January 30, 2019; Bundeskartellampt, Decision of December 22, 2015, B-9-121/13, *Online hotel booking platforms*; Bundeskartellampt, Decision of October 22, 2015, Case B6-57/15, *Online dating platforms*; see also "Bundeskartellampt initiates abuse proceeding against Amazon," published on November 29, 2018, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/29_11_2018_Verfahrenseinleitung_Amazon.html.

4 Margrethe Vestager, extract from speech held at the *Conference on shaping Competition Policy in the era of Digitisation*, Brussels, January 17, 2019.

5 Case COMP/M.7217, *Facebook/WhatsApp*, [2014] OJ C417/4, para. 164.

6 Commission, press release of December 6, 2016, IP/16/4284 in case COMP/M.8124, *Microsoft/LinkedIn*, [2016] C388.

7 Bundeskartellamt, "Background information on the Facebook proceeding," published on December 19, 2017, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6, accessed on January 30, 2019.

8 *Ibid.* question 3, page 2.

9 *Ibid.* question 3, page 2.

10 The German competition authority rendered the final decision on February 7, 2019. The decision was not yet published at the time of writing this article. In its press release, the German competition authority considered that Facebook's data processing terms, enabling the collection, merger and use of user data without valid consent, constituted an abuse of a dominant position justifying "far-reaching restrictions" on Facebook.

position? Are we there yet? Or are we still at a stage where data protection is ***just*** a "dimension" of competition law in the tech sector?

To answer these questions, we will examine whether a synergy exists between EU competition law and EU data protection law, which would allow competition enforcers to impose data sharing – as an access remedy – in abuse of dominance cases. We will first briefly describe the two theories of harm upon which the FCO relied (in its preliminary legal assessment) and then analyze a potential data sharing remedy through the lens of both EU data protection and EU competition law.

II. ACCESS TO DATA – A POTENTIAL REMEDY IN A DOMINANCE ANTITRUST INVESTIGATION AGAINST TECH GIANTS?

A. The FCO's Theories of Harm in the Facebook *Case*

1. Users Lose Control over Their Personal Data

The FCO's first theory of harm focuses on the users' loss of control over their personal data: namely that "users are no longer able to control how their personal data is used."[11] In essence, the FCO takes issue with the fact that Facebook is collecting user data from third party websites when these websites implement a Facebook "like button" – even if the user is not using these services or has actively objected to web tracking.[12] This enables Facebook to collect personal data from users of these websites without their knowledge and even against their explicit will.[13] In the FCO's preliminary assessment, Facebook's terms and conditions in this regard are neither justified under data protection principles, nor are they appropriate under competition law standards. The FCO therefore found that Facebook violated the fundamental right to informational self-determination – which is enshrined in the German constitution[14] – of its users, which ultimately harms consumers.

It is interesting that "unfair" data protection policies are considered by the German competition enforcer as anticompetitive conduct/abuse of a dominant company occurring under the data protection sphere. One could claim that – in parallel with its antitrust enforcement – the FCO is actually also enforcing an infringement of Article 6 GDPR (Lawfulness of processing) under antitrust rules. In particular, Article 6(a) GDPR provides that "processing shall be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes."[15] While the FCO refrains from expressly analyzing whether users have given their *explicit consent* or not in its preliminary assessment, it implicitly indicates that users have not given Facebook their consent for the acquisition of their data from third party websites, since users have lost control over their data.[16]

The preliminary assessment of the FCO is silent on what constitutes specific and actual consumer harm resulting from the loss of control over users' data. It remains to be seen whether the FCO will build a solid bridge between a data protection concept – loss of control over a users' data – and the competition law concept of consumer harm.

---

11 *Supra* note 7, question 7, page 4.

12 "If a third-party website has embedded Facebook products such as the 'like' button or a 'Facebook login' option or analytical services such as 'Facebook Analytics', data will be transmitted to Facebook via APIs the moment the user calls up that third party's website for the first time. These data can be merged with data from the user's Facebook account, even if the user has blocked web tracking in his browser or device settings." *Supra* note 7, "Background information on the Facebook proceeding," (2017), question 4, page 2.

13 "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." *Supra* note 7, "Background information on the Facebook proceeding," (2017), question 7, page 4.

14 The fundamental right to privacy is guaranteed by Art 1 in connection with Art 2 of the Grundgesetz.

15 Article 6(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

16 Contrary to the preliminary legal assessment, which did not mention the absence of user's consent, the President of the FCO stated in the press release accompanying the final (unpublished) decision that "The previous practice of combining all data in a Facebook user account, practically without any restriction, will now be subject to the voluntary consent given by the users. Voluntary consent means that the use of Facebook's services must not be subject to the users' consent to their data being collected and combined in this way." FCO press release "Bundeskartellamt prohibits Facebook from combining user data from different sources" available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3600108.

If the European Commission prosecuted the same case under EU competition law, the Commission might allege that "misleading" data protection policies are a violation of Article 102(a) TFEU, an abuse of market dominance that imposes "unfair trading conditions." This could be seen as a consequence of the *Astra Zeneca* jurisprudence, where the European Court of Justice found the company's conduct consisting in "deliberate" and "consistent" "misleading representations" and "misleading information" to be an unfair trading condition,[17] although it is not clear that this case law would support this conclusion. If the Commission follows this approach, dominant online platforms competing for the acquisition of personal data and offering services that infringe data protection rules could face antitrust liability for the conduct insofar as it can be proved that this behavior in the market harms consumers.

2. Foreclosure of Facebook's Advertising Customers

The FCO's second theory of harm is only briefly described and relates to Facebook's potential foreclosure of its advertising customers. The German authority is worried that Facebook "is becoming more and more indispensable for advertising customers" and that "there is *also* potential for competitive harm on the side of the advertising customers who are faced with a dominant supplier of advertising space."[18] The word "also" in the abovementioned sentence may indicate that the foreclosure of advertising customers is not the focus of the FCO's investigation.

In other words, what the FCO seems to be saying is that Facebook is not only collecting user data from third party websites without valid consent, but with the help of this data it generates specific user profiles – that no other platform is able to generate – which in turn enable Facebook to improve its targeted advertising activities. Therefore, the FCO's theory may be that Facebook's leverage in a "targeted advertising market" is a consequence of its "unfair" data protection terms and conditions. Some problems that could arise from this theory relate to the fact that data might not be a rival good, there may be reasonable substitutes to data, a reasonable substitute may be available for purchase or even for free, data may be useless without a know-how with regards to processing and analyzing it, etc. If the FCO's final decision elaborates on this theory of harm, it will signal a growing intersection of competition law and data protection law.

Another question is whether the foreclosure of Facebook's customers who want to buy advertising space would be solved through an "access to data" remedy? Would this approach enable customers to enter the relevant market and to compete? In this sense, we will now analyze whether an "access to data" remedy in an abuse of dominance case would be possible under competition and data protection laws.

For the FCO's first theory of harm regarding data subjects' loss of control over their data, it is quite difficult to imagine a robust competition law remedy. We will therefore explore a potential remedy for the second theory of harm, i.e. foreclosure of Facebook's advertising customers. For this purpose, we will look at a potential "forced" data access from both competition law and data protection perspectives.

B. Competition Law Scrutiny of the "Access to Data" Remedy

While in the U.S. there is no competition law basis for a forced access to data remedy where a company owns or controls relevant data, in the EU this can be envisaged under the ''essential facility" doctrine.[19] This doctrine can provide a competition law remedy when a dominant company refuses to grant access to data, e.g. to an intellectual property right, as in the *IMS Health* case.[20]

The EU courts have held that a refusal to grant access to data – more specifically to license a proprietary IP right - is abusive if it is imposed by a dominant company and (i) the data is indispensable to compete; (ii) the refusal to provide access to data eliminates effective competition in a secondary market; (iii) it prevents the emergence of a new product or limits technical development; and (iv) it is not objectively justified.[21] Therefore, the threshold for EU competition authorities to impose a "forced" access to data remedy is very high. It is doubtful, however, whether these conditions are going to be met in the German *Facebook* case. If the conditions are met, it remains to be seen to which extent the FCO may be willing to impose such a forced access to data remedy to enable advertising customers to compete, given that its principal theory of harm was actually the loss of control over users' data.

17 Judgment of December 6, 2012, *Astra Zeneca v. Commission*, C-457/10, EU:C:2012:770.

18 *Supra* note 7, question 7, page 4.

19 See Graef I., "EU Competition Law, Data Protection and Online Platforms," International Competition Law Series, Wolters Kluwer, 2016. See also Supreme Court of the United States, case 02-682, *Verizon Communications v. Trinko LLP*, where US Supreme Court held that a monopolist's unilateral refusal to cooperate with a rival is lawful where there is no history of a prior course of dealing.

20 Judgment of April 29, 2004, *IMS Health*, C-418/01, EU:C:2004:257.

21 *Ibid.* para. 38; Judgment of September 17, 2007, *Microsoft v. Commission*, T-201/04, ECLI:EU:T:2007:289, paras. 330–336.

Data as an indispensable input requires the existence of technical, legal, or even economic obstacles capable of making duplication impossible, or even unreasonably difficult.[22] It would therefore be necessary for the FCO to establish, at least, that it is not economically viable for Facebook's advertising customers to create an alternative facility at a scale comparable to that of Facebook. One could therefore argue that for Facebook's advertising customers, it is impossible to recreate the amount of data that Facebook possesses, given that Facebook has gathered such specific information (also from third-party websites) that it can divide its users in no less than 29,000 categories.[23]

The second condition would involve the fact that Facebook's refusal to supply access to data to advertising customers would eliminate effective competition from a secondary market, where Facebook is also present. In other words, if Facebook refuses to supply data to a customer that is advertising electronics, only in the situation in which Facebook would also be active in the electronics market and would try to reserve this market for itself by refusing to deal, would this be anticompetitive. This means that, under the current interpretation of case-law, Facebook can legitimately refuse to give access to its data to advertising customers and prevent them from competing in markets in which Facebook itself is not present (yet).

A forced data sharing remedy would therefore fail to satisfy the second condition of the essential facilities doctrine. However, one needs to bear in mind that these conditions are "created" through jurisprudence of the EU courts and are not set in stone.

The third condition requires that the refusal to give access to data prevents the development of a new product – but this condition has only been applied for refusals to license intellectual property rights.[24] It may make no sense to apply this condition in the present case, because advertising customers want to have access to Facebook's data specifically because they want to sell their products.

As for the forth condition, Facebook may invoke an objective justification to offset an alleged refusal to give access to its data to advertising customers. Objective justifications that were accepted by EU courts were capacity restraints in supply (*Commercial Solvents*),[25] or improper commercial behavior of the customer (*United Brands*).[26] The question also arises whether a forced data sharing remedy could also be anticompetitive in and of itself if the data reveals competitively sensitive information from the data provider.

Assuming that none of these could apply in the present case, Facebook may potentially invoke data protection law to offset the claim.

In this sense it is interesting to note a recent case enforced by the French Competition Authority, where it found that a company was dominant and ordered it to disclose customer data to its competitors, since the data was strictly necessary to ensure that competitors could effectively approach customers and compete.[27] Nonetheless, it also imposed an obligation on the dominant company to introduce a system on the basis of which its customers could be informed of such transfer and have the possibility to oppose it.[28] In other words, while the French Competition Authority imposed a forced access to data as a competition law interim remedy, it also ensured that there was an opt-out on data protection grounds.

Therefore, in this context we will discuss whether, at the EU level, data protection law could constitute an objective justification for offsetting a potential "access to data" remedy.

C. Data Protection Scrutiny of the "Access to Data Remedy"

Assuming that a forced data access remedy would be possible from a competition law perspective, could this be trumped by data protection law, i.e. the GDPR? If a competition authority would impose upon a dominant player an obligation to share part of the data it controls with its customers or competitors, could this company defend itself by claiming that this would run against its obligations under the GDPR? The answer is not clear cut.

22 Judgment of November 26, 1998, *Bronner*, C-7/97, EU:C:1998:569, para. 44.

23 Graef I. & Prüfer J. (2018), "Mandated data sharing is a necessity in specific sectors," Economisch Statistische Berichten, 103(4763), 298-301.

24 Judgment of September 17, 2007, *Microsoft v. Commission*, T-201/04, ECLI:EU:T:2007:289.

25 Judgment of March 6, 1974, *Commercial Solvents v. Commission*, joined cases C-6/73, C-7/73, ECLI:EU:C:1974:18.

26 Judgment of February 14, 1978, *United Brands v. Commission*, C-27/76, ECLI:EU:C:1978:22.

27 Autorité de la concurrence (Paris), *GDF Suez/Direct Energie*, Decision n° 14-MC-02, September 9, 2014

28 *Ibid.* para. 294.

The dominant company under investigation, i.e. the potential data provider, could argue that a **forced data sharing** means that personal data will not be processed fairly and in a transparent manner in relation to the data subject, and would therefore **run against its obligations under Article 5(a) GDPR** ("lawfulness, fairness, and transparency principle"). In addition, according to Article 15 GDPR, the dominant company would have to inform data subjects that their personal data is being transferred to another company, to which they have not given their consent.

It is also important to note that the GDPR does not contain any explicit provisions for a potential "forced" personal data transfer mechanism between two private companies, as a consequence of imposing such a remedy on a dominant company following a competition law investigation. Arguably, the company to which the data is being transferred, i.e. the data seeker (a customer or a competitor),[29] would not have any legal basis for processing the personal data, so it would need to seek consent of the respective data subjects, which would be a very cumbersome task. Contrary to the alleged dominant player, i.e. the original data controller, who is forced by competition authorities to transfer data, the data seeker would not be able to claim that "processing is necessary for compliance with a *legal obligation* to which it is subject" (Article 6(c) GDPR), because it would not be under any legal obligation to process the data.

On the contrary, we are assuming that it is the customer/competitor who wanted to get access to the data in the first place through his voluntary will. In this context, a customer/competitor who would want to get access to data withheld by a dominant player may argue that a valid legal basis for the data processing constitutes "his legitimate interest" of promoting his business. This would, however, be a far-fetched interpretation of Article 6(f) GDPR, which may provide an adequate legal basis for a lawful processing for the data seeker. Moreover, it is also unclear which role the data seeker will play in this scenario, i.e. whether it will be considered to be a sole controller or a joint controller. In sum, one could therefore argue that the GDPR is probably ill-equipped to support a potential "forced" data sharing remedy in an abuse of dominance case.

III. CONCLUSION

In today's digital economy, personal data has economic value and is an important parameter of competition. The dynamics of the online world seem to have caught some regulatory and legislative authorities off guard. Today's reality is that competition and data protection law increasingly intersect but Europe's brand-new data protection law, the GDPR, lacks any explicit provisions for a potential "forced" mechanism to provide access to data following the imposition of such an obligation by a competition authority.

Competition authorities seem to be enforcing data protection standards in antitrust cases, but data protection authorities may apply different standards. This may lead to additional complexity of a regulatory framework that is already quite burdensome for businesses. The FCO's decision in the German *Facebook* case is eagerly awaited. It may set an important precedent, since it is the first time that an infringement of data protection rules will be examined by a competition enforcer under abuse of dominance rules. The case makes clear that from now on companies will need to bear in mind that enforcing "*unfair*" data processing policies may potentially violate both competition law provisions as well as European data protection laws.

29 In our case, the "data seekers" would be Facebook's advertising customers.

FACEBOOK'S ABUSE INVESTIGATION IN GERMANY AND SOME THOUGHTS ON COOPERATION BETWEEN ANTITRUST AND DATA PROTECTION AUTHORITIES

BY PETER STAUBER[1]

1 Peter Stauber is Associated Partner in the Antitrust Practice Group of Noerr LLP (Berlin).

I. INTRODUCTION

Antitrust law and data protection have rarely been mentioned in the same breath. It is true that antitrust issues arising from Big Data have been on everyone's mind for quite some time. However, the data-related debate in antitrust law focused primarily on how data-driven business models may change the market and create new possibilities for restricting competition. Just three years ago, the Monopolies Commission, a think-tank of the German Federal Government, noticed that the collection of vast datasets has been assessed only from the viewpoint of market concentration on (online) advertising markets, while the importance of data for the development of new products and particularly data protection issues were not considered in any significant detail.[2]

Change came quickly. In March 2016, the German Federal Cartel Office ("FCO") initiated proceedings against Facebook for the alleged abuse of its dominant position on the market for social networks by requiring users consenting to very wide data collection practices.[3] Now, almost three years later, the FCO finished its investigation. With its decision of February 6, 2019, the FCO ordered significant changes to Facebook's data collection and usage practices.[4] If upheld on appeal,[5] the decision promises to establish new standards for data collection and data usage at least for market-dominant undertakings. Further, the FCO's *Facebook* investigation can be considered one of the first practical examples for close cooperation between a competition authority and data protection authorities in an investigation. Until now, data protection authorities were considered as being solely responsible for enforcing data protection regulations. One consequence of the *Facebook* investigation may thus be the emergence of parallel oversight by both data protection and antitrust authorities. This will raise – also from a constitutional point of view – questions on how to properly delimit the authorities' jurisdiction.

II. THE *FACEBOOK* INVESTIGATION AND THE FCO'S PROHIBITION DECISION

The FCO's investigation into Facebook concerned the potential abuse of its dominant position in the German market for social networks by applying unfair terms and conditions on the collection and use of Facebook users' personal data.[6] At the end of 2017, the FCO informed the public that it has submitted its preliminary findings to Facebook for their comments. Although these preliminary findings have not been made public, the press release[7] and an accompanying "Background information paper"[8] described the scope of the investigation and the (preliminary) competition concerns of the FCO in more detail than had been known before. Simultaneously with adopting its decision, of which a public, non-confidential version will be published within the coming months, the FCO published an updated "Background information paper" that provides more details.[9] On February 15, 2019, the FCO also published a case summary on the *Facebook* decision.[10]

The currently known contents of the FCO's decision provide interesting insights on the interaction between antitrust and data protection law as well as some surprising viewpoints, in particular in connection with the market definition.

2 See Monopolies Commission, Special Report 68: Competition policy: Challenges of Digital Markets, June 1, 2015, para. 110.

3 FCO, press release of March 2, 2016, English version available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.

4 FCO, case summary of February 15, English version available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf.

5 According to the case summary published by the FCO, Facebook has already appealed against the decision; cf. FCO, *supra* note 4, p. 12.

6 FCO, press release of March 2, 2016, English version available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.

7 FCO, press release of December 19, 2017, English version available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2017/19_12_2017_Facebook.html.

8 FCO, Background information paper on the Facebook proceeding, December 19, 2017, English version available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.html.

9 FCO, Background information paper on the Facebook proceeding, February 7, 2019, English version available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf.

10 FCO, *supra* note 4.

A. Summary of the FCO's Order

With its decision, the FCO prohibits Facebook from applying terms of service according to which Facebook users, in order to use the social network Facebook, have to grant their consent to the collection of their personal data not only on this social network itself, but also on Facebook-related applications (Instagram, WhatsApp, Oculus, and Masquerade), and on third party websites and apps that use Facebook Business Tools ("Like" and "Share" buttons), or analytical services from Facebook Analytics. In particular, Facebook is prohibited from combining personal user data collected on these "off-Facebook" websites and applications unless the users gave their voluntary consent. Users must be allowed to deny (or withdraw) their consent at any time without such denial/withdrawal affecting their possibility of using the Facebook social network. In order to comply with the order, Facebook is obliged to present the FCO within four months with its proposal for changes to Facebook's terms of service, explanatory data, and cookie policies. The prohibition will take effect within twelve months after the date of the decision. Given the FCO's restricted jurisdiction, its order applies only with regard to the data collection practices applied to private users residing in Germany.

B. Relevant Market and Facebook's Market Position

European[11] and German law[12] prohibit a market-dominant undertaking to abuse its market position. Thus, any assessment of an allegedly abusive market conduct requires identifying the affected market and establishing the market position of the undertaking under investigation.

1. Relevant Product Market

The *relevant product market* is usually defined as encompassing all products which are regarded by the consumer as interchangeable or substitutable in terms of their characteristics, prices, and intended use.[13] As a result of its assessment of various social media offerings, the FCO established the existence of a market for social networks[14] which is a distinct and separate market segment of the overall social media market. In this respect, the FCO took note that Google+ has essentially left this market[15] and thus, only some smaller German social network providers (studiVZ, meinVZ) were acknowledged as operators of competing social networks in this market.[16]

The FCO further ruled that professional social networks (LinkedIn, Xing), messaging services (WhatsApp, Facebook Messenger, Snapchat, etc.), or other media services such as YouTube and Twitter are not part of the relevant market. Although these services can (partly) substitute Facebook's functionalities, they serve different, complementary needs and thus, may not be considered as full substitutes.[17]

This reasoning concerning the boundaries of the relevant market were to be expected since they have already been considered by the European Commission in the merger control review of the *Facebook/WhatsApp* transaction.[18] While the Commission left open how to exactly define the affected market, the FCO had to take a decision – and it apparently opted for the narrower definition. This is hardly surprising, albeit some question marks remain since for some time Facebook appears to have lost popularity within the younger generations who instead prefer using Instagram, Snapchat, and similar services.[19] Further, in light of recent news that Facebook plans integrating its messaging services WhatsApp, Instagram, and Facebook Messenger,[20] one wonders how long the FCO's narrow market definition will be supported by the usage realities.

---

11 Art. 102 TFEU.

12 Sec. 19(1) ARC.

13 European Commission, Notice on the definition of relevant market for the purposes of Community competition law, OJ 1997 C 372, p. 3, 5.

14 Cf. FCO, *supra* note 4, p. 3 et seq.

15 As of February 4, 2019, it is no longer possible to open a Google+ account. On December 10, 2018 Google announced that due to serious bugs in Google+ APIs the consumer version of Google+ will be shut down in April 2019; cf. https://www.blog.google/technology/safety-security/expediting-changes-google-plus/.

16 Rather "were" since the operator of the social networks studiVZ/meinVZ declared its insolvency in September 2017.

17 Cf. FCO, *supra* note 4, p. 5.

18 European Commission, decision of October 3, 2014, COMP/M.7217 paras. 51 et seq. – *Facebook/WhatsApp*.

19 Pew Research Center, Social Media Use in 2018, March 1, 2018, http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.

20 New York Times, January 25, 2019, "Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger," https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html.

2. Relevant Geographic Market

Perhaps more surprisingly, the FCO seems to take the stand that the market for social networks is (only) national in scope.[21] In contrast, the European Commission held in its *Facebook/WhatsApp* decision that the geographic scope of the market for social networking services is EEA-wide "in line with a more conservative approach."[22] According to the case summary, this narrow scope of the geographically relevant market resulted from its main use to connect with people in the user's own country, special national user habits, and the lack of opportunities for supply-side substitution.[23]

This reasoning is somewhat perplexing. Usually, the *relevant geographic market* is defined by the area in which the relevant products or services are offered and in which the conditions of competition are sufficiently homogeneous.[24] It appears safe to assume that Facebook is accessible worldwide. Moreover, users can choose between at least 100 languages[25] for using Facebook without a reduction in the available functionalities. If the purpose of using a social network for staying in touch with friends in Germany were that decisive, one would expect that German-language focused social networks such as meinVZ/studiVZ had remained as relevant as in the mid-2000's. The counter-factual of the reality, i.e. Facebook's rise to become the most important social network in the EU and in Germany, in particular, may thus point to the importance of an at least EEA-wide, if not worldwide user base. Interestingly, the FCO uses the "size and the possibility to find the persons they want to be in contact with" in its reasoning for defining the scope of the product/service market. In light of this, it appears inconsequential to disregard the size of a social network's non-German user base as a relevant factor for choosing between rival social networks.

3. Facebook's Market Position

Under German law, an undertaking is considered to have a market-dominant position if it does not have competitors, is not exposed to any substantial competition, or has a paramount market position in relation to its competitors.[26] In assessing an undertaking's market position, the statute lists its market share as the first aspect to consider, and its financial strength as second.[27] In case that an undertaking has a market share exceeding 40 percent, German law provides for a (rebuttable) statutory presumption of market dominance.[28]

According to its case summary, the FCO's investigation established that Facebook, especially among daily active users, has a market share in Germany in excess of 95 percent and thus considers it being a "quasi-monopolist."[29] High market shares were also found when looking at monthly active users (> 80 percent) and registered users (> 50 perent), respectively.[30] In the opinion of the FCO, the amount of time spent by users on a social network is an important indicator of the network's success and thus the number of daily active users is considered as the decisive indicator for its market power.

In this connection, the FCO states that due to direct network effects, Facebook users are "locked in" and have extreme difficulties in switching to competing services. This appears to be an exaggeration. Indeed, it is very simple setting up an account at another social network (Google+, Reddit, etc.). The "difficulty" might thus better relate to the difficulty in finding a similar level of user activity, for example on Google+, or re-connecting with friends and acquaintances on a network that does not require users to reveal their true identity (e.g. Reddit, Tumblr). However, as the "boom and bust" of studiVZ, once the market-leading social network in Germany, and the parallel ascent of Facebook shows, the switching of a large user base from one network to the other is possible. However, such migratory movements do not happen frequently. According to the case summary, the possibility of a trend to withdraw from Facebook was also investigated. The FCO found that innovations on the internet are able to have disruptive effects, but in the case of Facebook any innovations of competitors only addressed certain functionalities and moreover,

21 Cf. FCO, *supra* note 4, p. 5.

22 European Commission, decision of October 3, 2014, COMP/M.7217 para. 67 – *Facebook/WhatsApp*.

23 FCO, *supra* note 4, p. 5.

24 European Commission, Notice on the definition of relevant market for the purposes of Community competition law, OJ 1997 C 372, p. 3, 5.

25 Information on this point varies, some sources state "over 100" available languages, others claim 142, cf. https://www.quora.com/How-many-languages-can-Facebook-support.

26 Sec. 18(1) ARC.

27 Sec. 18(3) no. 1, 2 ARC.

28 Sec. 18(4) ARC.

29 FCO, *supra* note 4, p. 6.

30 *Ibid.*

these competitive threats have been successfully addressed by Facebook.[31]

In summary, the FCO's position that Facebook enjoys a dominant position on the German market for social networks is not surprising, and it appears to be well reasoned. Even if the FCO adopted the Commission's viewpoint of an EEA-wide market for social networks, it does not appear far-fetched to assume that the FCO had arrived at the same result of establishing Facebook's market dominance.

C. Abusive Conduct

First, it appears important to note that the scope of the FCO's investigation was limited to the collection and use of user data collected "off Facebook," i.e. via "Like" and "Share" buttons embedded on third-party websites and apps, and by means of analytical services such as "Facebook Analytics."[32] For the time being, the FCO explicitly excluded from its investigation the examination of data collection practices on Facebook itself as well as the data collection policies of other Facebook-owned services, e.g. Instagram and WhatsApp.

As far as the use of "off Facebook" user data is concerned, the FCO ruled that Facebook's current terms and conditions are exploitative since they require that users consent to the collection, combination, and use of their personal data also on other Facebook-owned applications and on third party websites and applications even if the user has disabled web tracking.[33] In the opinion of the FCO, this wide scope of user consent requested from Facebook for the collection and use of their personal data violates data protection principles and in particular, Facebook's practices lack "*effective justification* […since it] *is neither required in order to fulfil contractual obligations nor does a balancing of interests result in the conclusion that Facebook's interests in data processing outweigh the users' interests*."[34] In this respect, the consent granted by users by accepting Facebook's current terms of service are considered ineffective since users had no choice than to consent to the "off Facebook" data collection in order to be able to use Facebook itself.[35]

Pursuant to German case law, the use of unfair general terms and conditions by a market-dominant undertaking may be qualified as abusive business conduct if, and to the extent, the legitimate interests of the dominant undertaking do not outweigh the legitimate interests of the counterparty,[36] i.e. the user of the social network Facebook. With regard to the latter, the FCO argues that both data protection law, as well as antitrust law, aim to protect individuals from the exploitation of their personal data by the opposite market side by safeguarding the users' right to choose freely when, by whom, and how their personal data may be collected and used. The FCO's reasoning mirrors the opinion of the Monopolies Commission, an independent think-thank of the German Federal government, that has advocated for an increased relevance of data protection law in antitrust assessments and called for sanctioning the "abuse of power through the breach of law."[37]

However, the purpose of antitrust law is to protect against restraints of competition and abusive behavior, but not supporting the enforcement of other legal norms, e.g. data protection rules. Otherwise there would be a risk that antitrust law is used to compensate for deficiencies in other laws and, respectively, for unsatisfactory enforcement by other authorities (e.g. data protection agencies). Accordingly, the European Commission held in its *Facebook/WhatsApp* decision that data protection concerns do not fall within the scope of European competition law.[38] Although the Commission's statement sounds rather clear, the more "inclusive" approach of the FCO appears to be more correct.

The assessment whether a given market conduct may qualify as abusive requires weighing the countervailing interests of the opposing parties. On Facebook's side, it appears obvious to consider their interest to gather as much user data as possible that allows for more tailor-made services for users and, obviously, also possibilities for more targeted advertisements. Thus, if Facebook's interests in obtaining personal data is (and should) be considered for its benefit, then it would be counterintuitive – and probably also wrong – not to consider the users' interests in

31 FCO, *supra* note 4, p. 7.

32 FCO, *supra* note 4, p. 12.

33 FCO, *supra* note 4, p. 7, 11 et seq.

34 FCO, *supra* note 4, p. 10.

35 FCO, *supra* note 4, p. 10. See also Art. 4 no. 11 GDPR.

36 Cf. Federal Court of Justice, decision of November 6, 2013 – KZR 58/11, NVwZ-RR 2014, 515, 520 – *VBL-Gegenwert I*; decision of June 7, 2016 – KZR 6/15, NZKart 2016, 328, 331 – *Pechstein*.

37 Monopolies Commission, Special Report 68: Competition policy: Challenges of Digital Markets, June 1, 2015, para. 110.

38 European Commission, decision of October 3, 2014, COMP/M.7217 para. 164 – *Facebook/WhatsApp*: "Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."

having some right to choose which data they want to hand over to whom and for which purpose. The FCO's focus on the collection and use of "off Facebook" user data thus appears to be not only plausible, but consequential since it leads to the question of whether Facebook's interest in collecting data on its users that are generated on third parties' platforms is similarly justified by Facebook's interest in generating tailor-made services and ads on Facebook. According to the FCO, the answer appears to be a clear "No." Only once a non-confidential version of the decision is published, it will be possible to review whether the FCO's standpoint might be more nuanced, allowing for exemptions, for example.

D. What comes next after the Facebook *Decision*

The FCO's decision requires Facebook to change its terms of service for users based in Germany within the next 12 months. Prior to that, within four months after the decision date, Facebook is obliged to present the FCO with an implementation plan setting out in detail the technical implementation of the obligations.[39]

However, Facebook has the possibility to appeal the FCO's decision and, according to the FCO's case summary, has already done so.[40] The appeal does not have a suspensory effect and thus Facebook would have to abide by the order unless it files an emergency appeal requesting a suspension of the order's effects for the duration of the proceedings.[41] Since Facebook indeed filed such an emergency appeal already,[42] a court decision containing at least a cursory review of the FCO's reasoning can be expected relatively soon within the next three months.

III. INTERACTION BETWEEN DATA PROTECTION AND ANTITRUST AUTHORITIES

If access to data is an essential factor for the competitive position of the company – as is the case with data-driven products such as social networks – the handling of personal data by a company is not only a case for data protection authorities, but also for antitrust authorities. If the question raised above of the inclusion of data protection assessments within the scope of abuse control is answered in the affirmative, the follow-up question on the relationship between data protection and antitrust authorities arises.

As already stated above, the FCO's Facebook investigation was conducted within the framework of an administrative proceeding.[43] As mentioned further, however, the FCO may switch to and, respectively, initiate administrative fine proceedings if it has sufficient reasons to believe that the seriousness of the abusive behavior requires a financial penalty as a proper sanction. Given that compliance with data protection provisions is at stake, data protection authorities may also become active and try initiating their own investigations. Accordingly, the following topics might become important for the affected undertakings.

First, fines for infringing data protection provisions may no longer be qualified as "small change," but rather as the (slightly) younger sibling of antitrust fines. Second, cooperation and information exchange between the FCO and data protection authorities will become more important, in particular since the latter will have significantly more experience in interpreting and applying the provisions of the GDPR. Lastly, and perhaps most importantly, if infringements of data protection rules may also qualify as market abuse within the meaning of Art. 102 TFEU, Sec. 18 et seq. ARC, this leads to the question whether undertakings are protected from parallel investigations and penalties by the *ne bis in idem* principle, i.e. a fine decision of one authority prevents the other authority from also imposing a fine.

A. Antitrust and Data Protection Fines

Through the GDPR, that entered into force on May 25, 2018, the provisions on financial sanctions for infringements of the GDPR were largely modeled after the respective antitrust rules. Previously, German data protection authorities could only sanction an undertaking with a fine of up to 2 million Euro. Based on the GDPR, the maximum fine now amounts to 20 million Euro. Moreover, undertakings may be sanctioned by a fine of up to 4 percent of worldwide turnover in the last business year. The similarity to the level of antitrust fines under European and German law are manifest: Under European law, the Commission may fine undertakings up to 10 percent of their worldwide turnover.[44] German law provides for

39 FCO, *supra* note 4, p. 12.

40 *Ibid.*

41 Cf. Sec. 64(1), 65(3) 1st sentence no. 2, 3, 3rd sentence ARC.

42 FCO, *supra* note 4, p. 12.

43 FCO, *supra* note 9, p. 1.

44 Art. 23(1), (2) 2nd sentence Regulation (EC) No. 1/2003.

the same maximum fine for undertakings, while it also allows for sanctioning individuals with a fine of up to 1 million Euro.[45]

B. Cooperation Between Authorities in Investigations

The 9th Amendment to the Act against Restraints of Competition, which entered into force in June 2017, established the legal basis for the cooperation between competition authorities and data protection authorities. Pursuant to Sec. 50c(1) ARC, Federal and state competition authorities and Federal and state data protection authorities may exchange information, including personal data, business, and trade secrets, insofar as necessary for fulfilling their duties, and use the information in their respective investigations and proceedings. The information exchange is not restricted by the type of investigation pursued by either authority, i.e. a data protection authority may make information that has been gathered in the course of administrative proceedings available to the FCO, and the FCO may use it for evidentiary purposes in administrative fine proceedings and *vice versa*.

It appears noteworthy in this respect that the provision not only does not require the authorities to inform the affected individuals and undertakings prior to, but neither after information has been exchanged. This might be seen as concerning. However, the receiving authority may not use information against individuals or undertakings if the information has been gathered by the supplying authority on the basis of seizure privileges unavailable to the receiving authority.[46]

C. Parallel Investigations and the "ne bis in idem" Principle

The possibility of parallel investigations by competition and data protection authorities raises the question of whether both authorities may adopt a fine decision against the affected undertakings.

Pursuant to the *ne bis in idem* principle, which is enshrined in the German constitution,[47] the Charter of Fundamental Rights of the European Union,[48] and the 7th Protocol to the European Convention of Human Rights,[49] a natural or legal person must not be penalized twice for one and the same cause of action.[50] According to the decision practice of the European Court of Human Rights, the *ne bis in idem* principle prohibits any prosecution resulting from a second offense where that offense is based on identical or substantially similar facts to the ones which were the basis for another offense.[51] The ECJ generally shares this approach. Accordingly, the *ne bis in idem* principle may be infringed if two investigations are pursued for the same acts, i.e. a set of concrete circumstances which are inextricably linked together, irrespective of the legal classification given to them or the legal interest protected.[52] On the other hand, the ECJ applies a slightly different standard in competition cases, i.e. the principle only applies if the facts and the offender are identical, and the legal interests protected are the same.[53]

If a competition authority may establish that a market dominant undertaking has abused its position by infringing data protection rules, the question arises whether a data protection authority may still investigate and sanction solely the data protection violation or whether it is barred due to the competition authority's decision. Based on the standard applied by the ECHR and the ECJ in non-competition cases, the answer should be "No" since the data protection authority's decision would be based on facts – as far as the data protection violation is concerned – that are identical to those underlying the competition authority's decision.

On the other hand, if the ECJ's stance for competition-related cases is followed, not only parallel investigations seem admissible, but also fine decisions by both the competition authority and the data protection authority. The prohibition to abuse a market-dominant position shall ensure that competition is not distorted and, more precisely, shall protect market participants on the opposite side of the market, the dominant

45 Sec. 81(4) 1st sentence ARC.

46 Sec. 50c(1) 2nd sentence ARC.

47 Art. 103(3) Base Law.

48 Art. 50 CFREU.

49 Art. 4 Protocol No. 7 to the ECHR.

50 Also known as double jeopardy doctrine in common law jurisdictions.

51 Cf. ECHR, Sergey Zolotukhinv ./. Russia [GC], no. 14939/03, ECHR 2009, paras. 82 et seq.

52 Court, judgment of November 19, 2010, case C-261/09 para. 39 – *Gaetano Mantello*.

53 ECJ, judgment of January 7, 2004, joined cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P para. 338 – *Aalborg Portland et al. / Commission*.

undertaking's competitors (if any), consumer welfare, and the Common Market.[54] In contrast, data protection rules protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[55] Thus, one may argue that the two areas of law serve different legal interests, and therefore parallel sanctions by a competition authority and a data protection authority may not violate the *ne bis in idem* principle. Even though this appears plausible, both fine decisions would still have the infringement of data protection laws as their (sole) substantive basis.

German law solves such situations by a "first come first served" general rule which determines the authority that shall be competent for conducting administrative fine proceedings if the subject matter could be investigated and sanctioned by several authorities. More precisely, the first authority having interviewed the person concerned and, respectively, to whom the police have sent the file after an interview led by the police shall be competent for proceeding with the investigation.[56] Accordingly, if an alleged infringement of data protection laws is investigated first by a data protection authority with the aim of imposing a fine once the infringement has been established, then this would block a parallel (or subsequent) administrative fine proceeding by the FCO. Nevertheless, the primary authority would still have to consult with the other potentially competent authorities, e.g. the FCO, before concluding its investigation.[57] Further, the primary authority may also agree with another potentially competent authority for transferring the case to the latter if such a transfer increases efficient case handling or for other justified reasons.[58]

The aforementioned rules however only apply for administrative *fine* proceedings, i.e. where proceedings are concluded with the imposition of a financial penalty. Accordingly, if one of the competent authorities intends to investigate an infringement with the aim of imposing monetary sanctions, the other authority may still conduct its own investigation within the framework of a purely administrative proceeding. In case of the latter, the authority may then only adopt cease and desist orders or request the infringing party to undertake specific measures. Similarly, the *ne bis in idem* principle is not relevant if neither one of the authorities opts for an administrative fine proceeding. Since this may lead to diverging or even contradictory interpretations of legal provisions, coordination between the authorities will remain necessary.

IV. CONCLUSION

After previous statements by the FCO promising an earlier conclusion of the *Facebook* investigation, the decision day has now come. Although the materials published by the FCO so far concerning its decision are significantly more detailed than usual, a number of questions remain and might be answered only once a non-confidential version of the decision has been published. Regardless, the available information already provides more than a glimpse into the FCO's view on the interaction between data protection rules and antitrust law. Although one could argue that the FCO's opinion is a Germany-specific divergence, a more cautious approach may be well advised. As one of the larger markets in Europe, developments in data protection laws usually also affect other countries and may also influence the viewpoint of data protection and antitrust authorities in other jurisdictions. Companies with data-driven business models may thus be well advised to review their data collection and use policies, in particular if they consider themselves having a significant market position in their respective fields.

54 Cf. Fuchs/Möschel in Immenga/Mestmäcker, European Competition Law, 5th ed. 201, Art. 102 paras. 4 et seq.

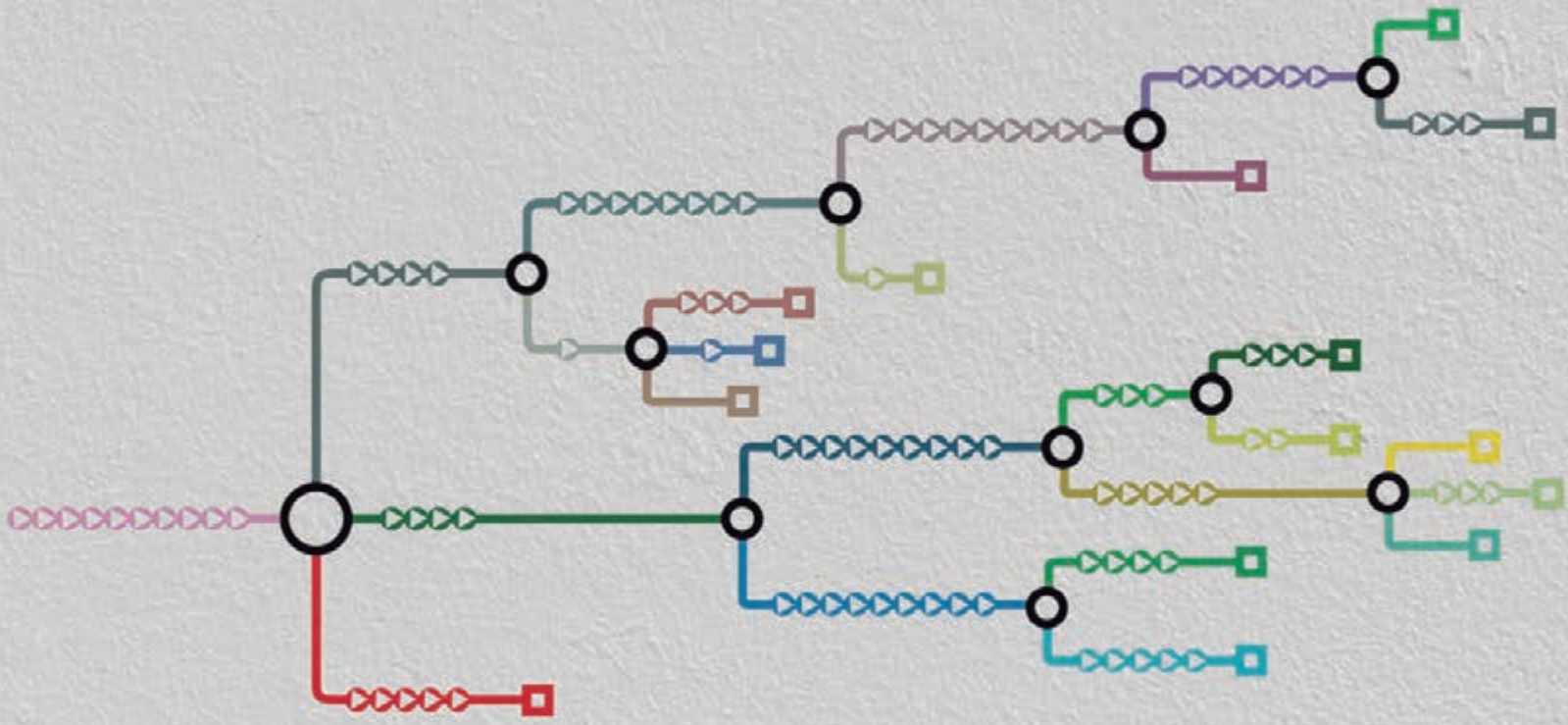
55 Cf. Art. 1(2) GDPR.

56 Sec. 39(1) 1st sentence German Act on Administrative Offenses (AAO).

57 Sec. 39(2) 2nd sentence AAO.

58 Sec. 39(2) 1st sentence AAO.

ANTITRUST AND DATA PROTECTION: A TALE WITH MANY ENDINGS



BY FILIPPO MARIA LANCIERI[1]

1 JSD Candidate, The University of Chicago Law School. Contact: filippolancieri@uchicago.edu.

I. INTRODUCTION

The rise of the data economy is bringing about many new challenges to antitrust law. As this edition of the Competition Policy International Antitrust Chronicle attests, one of the most debated concerns the potential interconnection between competition and data protection policies. This possibility is giving rise to a range of thought-provoking and meaningful contributions from diverse stakeholders.[2] This debate is also quickly moving from theory to practice. Cases and concerns involving the competitive effects of large datasets are multiplying – the best example being the Bundeskartellamt's recent condemnation of Facebook's data collection practices in Germany.[3] All in all, it is safe to say that as the data economy engulfs different markets and more countries strengthen data protection regulations, the more important it will be to delineate boundaries for the relationship between antitrust and data protection policies.

This contribution, which is largely based on a longer article published in the Journal of Antitrust Enforcement, aims to take a step back from this debate to argue that politics and sociological preferences will probably lead different jurisdictions to reach distinctive conclusions on what are the boundaries between competition and data protection.[4] It does so by looking at the foundations of antitrust and data protection policies in the United States and in the European Union as examples of how cultural attributes may impact such delimitations. Finally, it discusses how the European antitrust toolkit, when combined with European anxieties regarding data accumulation, enables the EU to become a leading jurisdiction in a push towards a more meaningful convergence of antitrust and data protection – or at least for the aggressive enforcement of antitrust policies in markets where data plays a crucial role.

In order to do so, this contribution is divided in four sections, the first being this brief introduction. The second discusses the foundations of current European and American data protection and antitrust policies. The third discusses how these differences may impact a potential convergence of both policies. The fourth briefly concludes.

II. THE FOUNDATIONS OF EU AND U.S. DATA PROTECTION AND ANTITRUST POLICIES

Despite innumerous pushes for harmonization over the years, the EU and the U.S. policies towards data protection and antitrust enforcement maintain different foundations and goals.

Firstly, one can look at the origins and current structure of the EU and the U.S. data protection policies.[5] The EU proto-federal data protection framework evolved mostly from a German/French culture of privacy protection as an inalienable right aimed at safeguarding personal honor against invasions by private third-parties (such as tabloids). These broad rights are enshrined, amongst others, in Articles 7 and 8 of the EU Charter of Fundamental Rights and translated by the General Data Protection Regulation in a complex system of regulatory agencies and processes that safeguard those interests. All in all, EU data markets are overseen and regulated by national and EU-wide data protection regulators and other institutions that impose limits on how parties obtain, process, publish, transfer and/or retain citizens' data and allow authorities to impose hefty fines in case of violations.[6]

Data markets behave differently in the US, where citizens have not historically been seen as "data subjects" protected by direct regulation, but mostly as "online consumers." The U.S.'s limited federal regulations on data protection focus primarily on public databases (e.g. the Privacy Act) and derive from a concept of privacy protection based on underlying values of self-government and self-determination where the Government, not private parties, is the main threat to one's liberties. The protection of privacy then meant safeguarding a sphere of private deliberation

2 See European Data Protection Supervisor, Preliminary Opinion of the European Data Protection Supervisor: Privacy and Competitiveness in the age of big data - The interplay between data protection, competition law and consumer protection in the Digital Economy (2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (last visited Jan 12, 2019); Maureen K. Ohlhausen & Alexander Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 Antitrust Law J. 121–156 (2015).

3 For example, the European Commission opening a preliminary probe against Amazon to investigate concerns regarding misuse of merchants' data, or the phase-II clearing of the Apple-Shazam acquisition – again due to data accumulation concerns; See also Bundeskartellamt, Bundeskartellamt prohibits Facebook from combining user data from different sources (2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3591568 (last visited Feb 7, 2019).

4 Filippo Maria Lancieri, *Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift*, J. Antitrust Enforc. 1–27 (2018).

5 This is a rough summary. For a more in depth view, see *Id.* pg. 4-7 and the references therein.

6 Something that is quickly starting to materialize, as shown by the first fines issued by the French and German data protection authorities. See Chris Fox, *Google hit with £44m GDPR fine*, January 21, 2019, https://www.bbc.com/news/technology-46944696 (last visited Jan 21, 2019); Tim Wybitul, Wolf-Tassilo Bohm & Isabelle Brams, German GDPR Fine Proceedings Conclude Favourably for Defending Company Global Privacy & Security Compliance Law Blog (2018), https://www.globalprivacyblog.com/privacy/german-gdpr-fine-proceedings-conclude-favourably-for-defending-company/ (last visited Jan 21, 2019).

against a growingly intrusive Federal investigative apparatus.[7] When combined with an expansive policy towards the protection of freedom of speech, including corporate speech, this framework restricted data protection regulation to some handpicked industries (health care, credit reporting, video rental and others). Personal data is mostly an asset that can be freely traded in private transactions, subject only to traditional limitations typically applicable to other private contracts. Indeed, the Federal Trade Commission, the U.S.'s most important data authority, lacks express powers to regulate data protection and has no fining authority – its actions are based on a common-law extension of its general mandate to protect consumers from unfair and deceptive acts.[8]

A less wide but equally important divergence exists between EU and U.S. competition protection policies.[9] Modern U.S. antitrust law still reflects much of the Chicago School's view that antitrust policy should maximize allocative efficiency and require clear evidence of consumer harm lest incurring in costly false positives. Under this approach, in which dynamic competition is the main driver of consumer welfare, markets are seen as typically self-correcting in the medium to long-term. As a result, the U.S. accepts as legal the charging of supra-competitive prices by a legitimate monopolist. Even more importantly, any analysis of unilateral conduct requires a rule-of-reason approach that is heavily built on economic evidence and imposes a high-burden of proof against any plaintiff trying to bring an abuse of dominance claim.[10] EU policy, on the other hand, reflects at least partially German Ordoliberalism views where competition protection plays both an important economic and political goal. This requires a strong state whose role is to open markets, keep these markets open to competition, and, if this process has failed, to act so as to regulate dominant companies, requiring them to behave at least partially as if they are in a competitive market. This dynamic empowers regulators to take action against dominant companies in general, be it through direct sectoral regulation or through more general abuse of dominance claims.

Rather than being merely theoretical, the distinctions outlined above impact both jurisdictions' antitrust policies against dominant companies in five important aspects (at least in what it relates to the possible interconnection between competition and data protection): (i) lower thresholds for the characterization of dominance in the EU when compared to the U.S.; (ii) a general view in the EU that dominant firms may have "special responsibilities" towards its competitors and the market in general; (iii) a more legalistic approach to unilateral behavior in the EU, in particular in how to characterize anticompetitive harm; (iv) a general prohibition in the EU against exploitative abuses that finds no parallel in the U.S.; and (v) a growing importance in the EU of looking at restrictions to freedom of choice as a potential anticompetitive harm.

It is not the goal of this brief summary to claim that one system is better than the other. Indeed, while the more market-oriented approach in the U.S. may lead to less legal protections when compared to the EU, it may also be one of the reasons why American companies are leaders in the data economy, significantly ahead of their EU counterparts. Rather, a comprehension of how and why different jurisdictions shape their data protection and competition policies may enable us to also better understand why discussions around a convergence between such policies is not necessarily bound to produce equal results. This is what the next section addresses.

III. ANTITRUST AND DATA PROTECTION: INTERNATIONAL CONVERSION OR DIVERGENCE?

The enforcement of any public policy is not done in a vacuum, but rather reflects fundamental preferences and political priorities of a given society.[11] These preferences impact enforcement in many ways: from the different legal framework in which agencies operate, passing by the specific reasoning of an agency staff member, and up to the complex system of political capital accumulation and expenditure that dictates part of the enforcement priorities of any regulator.[12]

The same process should come into play when regulators are faced with the challenge of considering a potential approximation between antitrust and data protection policies. Rather than following a previously defined recipe, policymakers will need to evaluate both the political implications of their choices and the toolkits available to them. Both variables are unique to each jurisdiction. Therefore, this process will most likely lead to some important divergences across the world. A comparison between the EU and the U.S. helps to exemplify why this is so.

---

7 For an example of the most recent iteration of this debate, see the recently decided Supreme Court decision *Carpenter v. U.S.*, 138 S.Ct. 2206 (2018)., discussing whether the government needs a warrant to obtain historical location data from cell-sites.

8 See Daniel J. Solove & Woodrow Hartzog, *The FTC and the new common law of privacy*, Columbia Law Rev. 583–676 (2014).

9 This is equally a rough summary. For a more detailed analysis see Lancieri, *supra* note 4. pg. 7-10 and references therein.

10 As seen by the recent Supreme Court decision in *Ohio et al vs. American Express Co et al*, 138 S.Ct. 2274 (2018).

11 For an analysis of how this process impacts competition policy, see Ariel Ezrachi, *Sponge*, 5 J. Antitrust Enforc. 49–75 (2016).

12 See David A Hyman & William E Kovacic, *Why Who Does What Matters: Governmental Design and Agency Performance*, 82 Geo Wash Rev 1446 (2013).

Starting with the toolkit, the historical evolution of the EU's competition protection regime places it in a unique position to incorporate some key concerns of data protection regulations. Abuse of dominance investigations against data companies have normally faced some significant hurdles in the U.S., as the multi-sided business-model of data giants defies the tools traditionally employed in market definition, assessment of market power and the calculation of efficiency, exclusion and consumer harm. For example, in a landmark decision that one hopes is largely ignored by other Courts, the Northern District of California dismissed an antitrust claim against Google under the allegation that free services prevent the finding of: (i) any relevant market that serves the purposes of antitrust law; or (ii) any form of consumer harm.[13]

The European Commission and national competition authorities, however, operate in a more flexible framework. European authorities may define relevant markets in a more conservative manner (e.g. a market for comparison shopping services that excludes Amazon) and presume dominance at market shares as low as 40 percent. They may also affirm a special obligation of dominant firms to consider the impact their actions have on the market as a whole and largely presume harm to consumers as a result of harm to smaller competitors. Even more importantly, EU authorities have the power to bring cases for exploitative abuses, or pure appropriation of consumer surplus, that find no counterpart in the U.S. This enables authorities to open antitrust cases against practices that are at the core of data protection regulations – excessive data accumulation or retention as a result of excessive market power. In other words, a major change in U.S. antitrust policy would be necessary for authorities to bring a case that clearly bridges antitrust and data protection policies. No such change is necessary in the EU.

One can tell a similar story about the political environment that instructs antitrust and data protection policymaking in both Europe and the U.S. General European concerns about corporate power and data accumulation mean that many European authorities gain political capital when they take action against data giants.[14] Similar actions in the U.S. imply an expenditure of such political capital that may be better used in other areas (such as concerns about the increase in horizontal shareholding amongst competitors). Indeed, the lack of any meaningful new regulatory initiative or enforcement action against data companies despite years of turmoil reflects, at least in part, the fact that these companies remain largely popular in America.[15]

Given all these foundational differences, it is unsurprising that the first well-known investigation clearly bridging the topics of antitrust and data protection is the Bundeskartellamt case against Facebook for exploitative abuses involving data collection. For historical reasons, Germans lead Europeans in terms of wariness towards industrial concentration and data accumulation (Germans were also among the first to impose a GDPR fine). While the European Commission is yet to take such a bold step, it is also leading the world in the analysis of the antitrust implications of large datasets, be it in merger review (e.g. *Facebook/WhatsApp*, *Microsoft/LinkedIn*, or *Apple/Shazam*) or, more recently, in abuse of dominance (with the newly opened *Amazon* probe).

Even more interesting, however, is to use the same framework to envision the evolution of the data protection/competition intersection in other jurisdictions around the world. As an example, one may look at Brazil and China, two major developing countries with active antitrust regulators that will probably end up following different paths.

The Brazilian antitrust regime largely trails that of the EU. Brazil has a history of abuse of dominance investigations against a multitude of companies, many operating in data intensive markets – even if these investigations are not data-related (sectors include electronic payments, telecommunications, online search and healthcare). Brazil also has a constitutional right to privacy and revamped its data protection regime in 2018, adopting a system modeled after the EU. Amongst its similarities, the new Brazilian legislation requires clear and unambiguous consent, affirms rights such as data minimization or portability and foresees the creation of a data protection regulator with strong oversight powers and the ability to impose fines.[16] On the other hand, even if in a growing trend, abuse of dominance investigations are yet to become a major focus of

13 See *KinderStart.com LLC v. Google, Inc.*, C 06-2057 JF (N.D. Cal. March 16, 2007).

14 Commissioner Vestager, for one, has accumulated so much political capital that The Economist, amongst others, is openly promoting her as a good contender for the presidency of the European Commission – in great measure because of her crackdown against U.S. data giants.. See Margrethe Vestager, bane of Alstom and Siemens, could get the EU's top job, The Economist, 2019, https://www.economist.com/europe/2019/02/07/margrethe-vestager-bane-of-alstom-and-siemens-could-get-the-eus-top-job (last visited Feb 7, 2019).

15 Even if, finally, some change seems to be taking place. See, for example, Tony Romm et al., *"It's about time": Facebook faces first lawsuit from U.S. regulators after Cambridge Analytica scandal*, Washington Post, December 19, 2018, https://www.washingtonpost.com/technology/2018/12/19/dc-attorney-general-sues-facebook-over-alleged-privacy-violations-cambridge-analytica-scandal/ (last visited Jan 19, 2019). and Tony Romm & Elizabeth Dwoskin, *U.S. regulators have met to discuss imposing a record-setting fine against Facebook for privacy violations*, Washington Post, January 18, 2019, https://www.washingtonpost.com/technology/2019/01/18/us-regulators-have-met-discuss-imposing-record-setting-fine-against-facebook-some-its-privacy-violations/ (last visited Jan 21, 2019).

16 Even if this creation has been somewhat contentious. It was vetoed by former President Michel Temer for a potential unconstitutionality and then reinstated by him through a new Law that is currently under analysis by the Brazilian Congress.

Chinese antitrust regulators.[17] China also diverges from Brazil in data protection. Aiming to become the "Saudi Arabia" of data, the Chinese government is encouraging the creation of vast databases, as shown by the development of the Chinese Social Credit System or the government's close alignment with Chinese data giants in the hope that they become leaders in Artificial Intelligence.[18]

It would not be far-fetched, then, that Brazilian competition authorities scrutinize more closely data-intensive companies than their Chinese counterparts. Or, even more importantly, that in this process Brazilian regulators incorporate some traditional data protection concerns, such as those related to excessive data gathering and retention or data processing not aligned with original user consent. In doing so, they would reflect preferences and political priorities of Brazilians that are not shared by the Chinese.[19]

IV. A TALE WITH MANY ENDINGS

The world economy is still in the early stages of the data revolution. The forthcoming adoption of 5G technologies and the quick rise of the Internet of Things that should follow will only deepen debates about what role data generation, processing, and accumulation play in a modern economy. Antitrust authorities perform a crucial role as market gatekeepers and will join data protection regulators in defining boundaries for data uses by private companies. It is likely, then, that we are also still in the early stages of the discussions on what are the borders between antitrust and data protection policies.

If the analysis herein is correct, what we may see is that like in many other areas (e.g. labor or industrial policy), the additional complexities created by the interaction of antitrust and data protection will lead to further international divergence in antitrust enforcement. This is already the case when one looks at Europe and the United States: where the European Commission and national regulators are pushing boundaries, we are yet to see any meaningful change in the U.S. It will also likely be the case when one looks at Brazil and China – with Brazilian antitrust authorities pushing for more strict enforcement against data companies than their Chinese counterparts. One can imagine that a range of other jurisdictions will adopt their own solutions, sitting somewhere in between the EU, Brazil, the U.S., and China. Rather than leading to a single, cohesive solution, this interaction will lead to a tale with many endings.

17 According to some reports, Chinese authorities have decided a total of only 12 abuse of dominance cases, mostly in areas also directly regulated by the government. See Susan Ning, China Dominance – Getting The Deal Through Getting The Deal Through (2018), https://gettingthedealthrough.com/area/10/jurisdiction/27/dominance-2018-china/ (last visited Jan 12, 2019); John Yong Ren, Wesley Wang & Schiffer Shi, China - Abuse of Dominance -The Asia-Pacific Antitrust Review 2018 Global Competition Review (2018), https://globalcompetitionreview.com/insight/the-asia-pacific-antitrust-review-2018/1166696/china-abuse-of-dominance (last visited Jan 12, 2019).

18 See CHINA MAY MATCH OR BEAT AMERICA IN AI, The Economist, 2017, https://www.economist.com/business/2017/07/15/china-may-match-or-beat-america-in-ai (last visited Jan 12, 2019). For an excellent analysis of the Chinese Social Credit System, see a paper by a recent graduate of UChicago's JSD program, Xin Dai, *Toward a reputation state: the social credit system project of China* (2018).

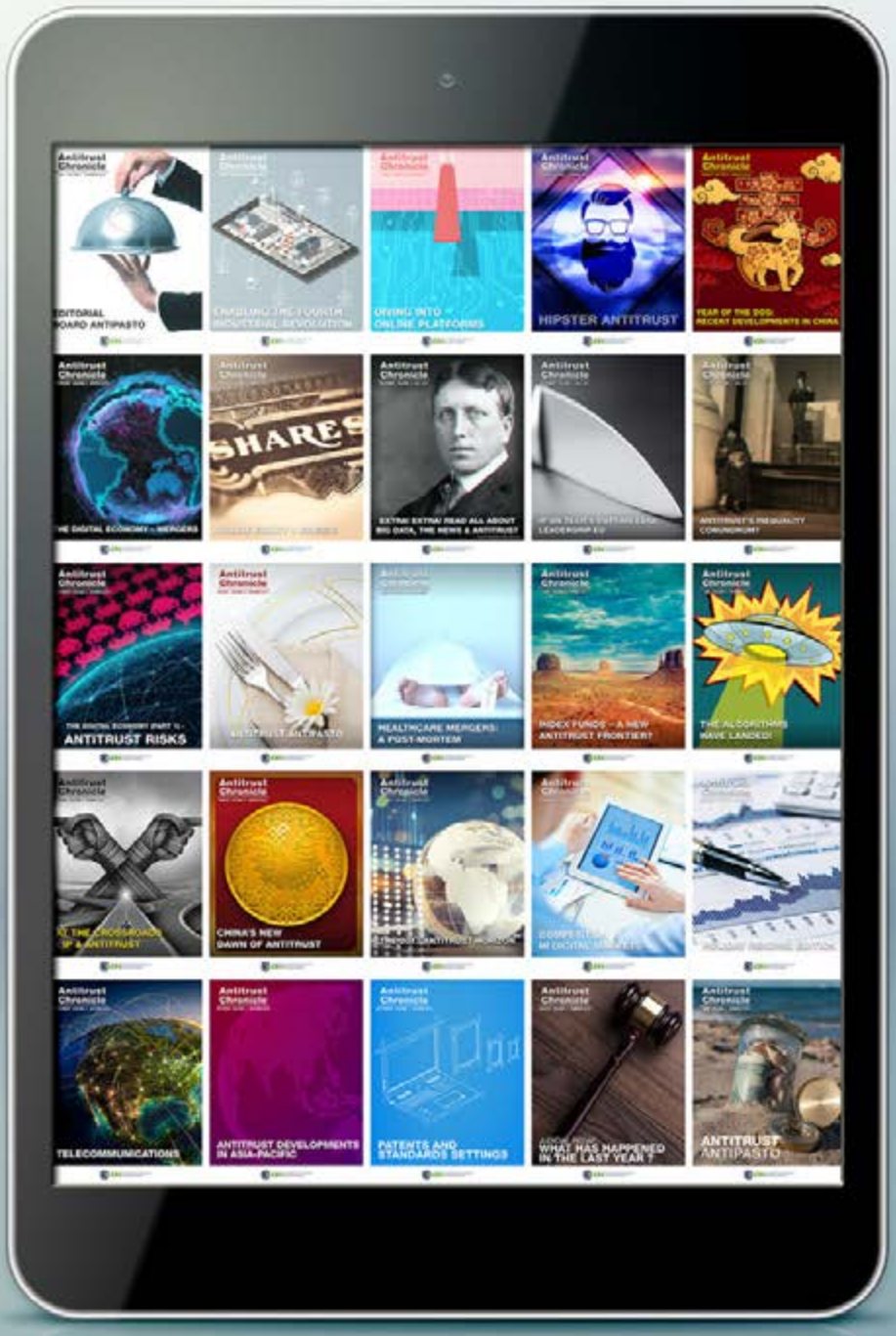
19 This is assuming that countries will maintain a single, cohesive and rational antitrust system. Another possibility is that antitrust systems fragment to reflect industrial policy considerations. This concern, however, is not unique to the data economy. Moreover, if this is the case, the rethinking of what role, if any, antitrust plays in an international context will have to be much deeper and antitrust itself will probably lose status as public policy.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 20,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.




CPI
COMPETITION POLICY
INTERNATIONAL