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 BUTTARELLI¹



CPI ANTITRUST CHRONICLE FEBRUARY 2019

CPI Talks...
...with Terrell McSweeny



This is not an Article on Data Protection and Competition Law

By Giovanni Buttarelli



Privacy and Competition: Friends, Foes, or Frenemies?



By Maureen K. Ohlhausen





Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision By Justus Haucapy



The German *Facebook* Case – Towards an Increasing Symbiosis Between Competition and Data Protection Laws?



By Dr. Jörg Hladjk, Philipp Werner & Lucia Stoican





Antitrust and Data Protection: A Tale with Many Endings
By Filippo Maria Lancieri



Visit www.competitionpolicyinternational.com for access to these articles and more!

CPI Antitrust Chronicle February 2019

www.competitionpolicyinternational.com Competition Policy International, Inc. 2019° Copying, reprinting, or distributing this article is forbidden by anyone other than the publisher or author.

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." 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 compa-

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.

nies 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

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.

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.

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 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.

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

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.

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 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.

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.

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.



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.

