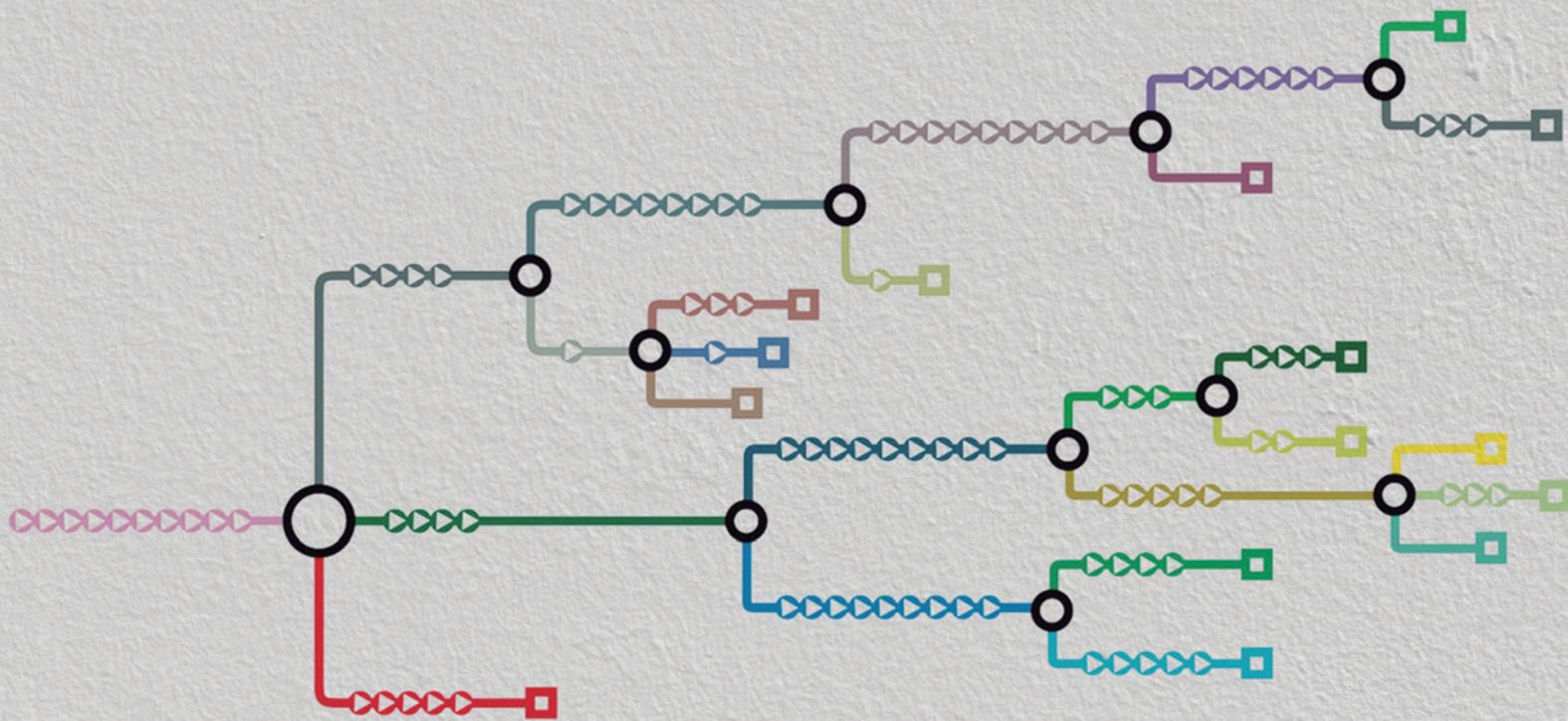


ANTITRUST AND DATA PROTECTION: A TALE WITH MANY ENDINGS



BY FILIPPO MARIA LANCIERI¹



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

CPI ANTITRUST CHRONICLE

FEBRUARY 2019

CPI Talks...

...with Terrell McSweeney



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



The Brazilian Data Protection Policy and its Impacts for Competition Enforcement

By Vinicius Marques de Carvalho & Marcela Mattiuzzo



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

By Justus Haucap



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

By Dr. Jörg Hladjk, Philipp Werner & Lucia Stoican



Facebook's Abuse Investigation in Germany and Some Thoughts on Cooperation Between Antitrust and Data Protection Authorities

By Peter Stauber



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. 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.

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_competition_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).

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

Despite innumerable 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 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.

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).

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).

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.

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

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).

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

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 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

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.

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.

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.



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.

