THE UNIVERSITY OF CHICAGO

ESSAYS IN THE REGULATION OF DIGITAL MARKETS

A DISSERTATION SUBMITTED TO

THE FACULTY OF THE LAW SCHOOL

IN CANDIDACY FOR THE DEGREE OF

DOCTOR OF JURISPRUDENCE

BY

FILIPPO MARIA LANCIERI

CHICAGO, ILLINOIS

AUGUST 2021

DEDICATION

To Claudio, Filippo, Ruth and Evenylde: you are eternally my main role models.

To Bia and Fred: your love and support made this dream a possibility.

To Pietro and Francesca: above all, you are my best friends.

And to Francine: I am always just trying to keep up with you.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

Dissertations are born of fire, the result of a long and lonely daily struggle with our ideas. Still, this dissertation would never have materialized if not for the support of many incredibly people that I had the privilege of interacting with over these past years (listed in alphabetical order).

The group certainly starts with my dissertation supervisors Lior Strahilevitz and Randy Picker, who I admire as both incredible scholars and, more importantly, individuals, and who steered me through the many challenges of this long process. Yet, it does not stop there, as I was privileged enough to have an "Extended Supervision Committee" of remarkable University of Chicago scholars that include: Adam Chilton, Guy Rolnik, Lisa Bernstein, Luigi Zingales, Omri Ben-Shahar, Tom Ginsburg, Travis Crum and William Hubbard (among others). In different ways and capacities, all of you (Lior and Randy included, of course) guided me when I needed guidance, comforted me when times were tough, uplifted me when needed and opened doors whenever possible. I will never be able to repay your kindness and attention and it is hard to express in words how much you have shaped me both as a person and as an academic. I promise to do my best to proudly carry the UChicago banner throughout the rest of my career.

This list, however, certainly includes additional people. A special mention goes to my long-time mentor Caio Mario Pereira Neto, who not only made me believe that a J.S.D. was a possibility, but also guided me throughout the process and even co-authored one of the chapters of this dissertation. I am also thankful to Anu Bradford, Fiona Scott Morton, Florence G'Sell, Joshua Tucker and Nicolo Zingales (among many others).

Finishing a J.S.D., however, requires not only work and mentoring but also friendship and love: the world sees the articles and the academic conferences, but it does not see the many secluded (and, in Chicago, particularly cold!) weeks and weekends when you are just feeling

overwhelmed and ready to give up. It goes without saying how important my family was throughout this process: Bia, Fred, Pietro and Francesca—we were physically apart but never distanced; Francine, probably the best part of this whole process was making sure that we will always be together—and joining Wicher, Mieke, Willem and Quirijn as a member of the van den Brandeler Family.

I was also incredibly fortunate to have many colleagues and others who honored me with their friendship. These include Asher Qazi, Asher Schechter, Barbara Marchiori, Chris Wheat, Emilie Aguirre, Jana Kaspervic, Krithika Ashok, Nino Guruli, Patricia Sakowski, Rachel Piontek, Ramon Feldbrin, Rodrigo Karolczak, Ryan Sakoda, Sannoy Das, Sebastian Burca, Simone Cavallaro, Shubho Roy, Weijia Rao, multiple friends from my LL.M. class as well as other LL.M. classes and many others.

Finally, each of my essays greatly benefited from feedback by multiple scholars from the University of Chicago and elsewhere. These are acknowledged below.

First Essay: Digital Protectionism? Antitrust, Data Protection and the EU/US Transatlantic Rift

I would like to thank Randal Picker, Lior Strahilevitz, Lisa Bernstein, Daniel Sokol, Ariel Ezrachi, Lars Kjølbye, Thorsten Schiffer, Riccardo Siemens, Patrick Todd, two anonymous reviewers, participants of the University of Chicago Legal Scholarship Workshop, participants of the 12th ASCOLA Conference, participants of UChicago's JSD Colloquium and participants of the 4th ASCL YCC Workshop on Comparative Business and Financial Law for interesting discussions and comments. I would also like to thank Latham & Watkins LLP for kindly accepting me as a visiting lawyer in their Brussel's office for an internship while writing this piece.

Second Essay: Narrowing Data Protection's Enforcement Gap

Above all, I would like to thank Professor Caio Mario Pereira Neto for honoring me as a co-author of this project. I would also like to thank Peter Alexiadis, Dennis Carlton, Damien Geradin, Alison Jones, Renato Nazzini, Randal Picker, Fiona Scott Morton, Lior Strahilevitz, Patrick Todd, participants in the University of Tilburg Law and Economics Center (TILEC) seminar series, participants of the 14th ASCOLA conference, as well as participants in a seminar held at the King's College London, for invaluable feedback and/or comments on earlier versions of this article. I also thank the *Antitrust Law Journal* reviewers and editors for excellent and insightful comments that helped to greatly improve the article.

Third Essay: Towards a Layered Approach to Relevant Markets in Multi-Sided Transaction Platforms

I would like to thank Lior Strahilevitz, Omri Ben-Shahar, Lisa Bernstein, Adam Chilton, William Hubbard, Brian Leiter, Travis Crum, Ari Ezra Waldman, Spencer Smith, Nicolo Zingales, Julian Nowag, Emilie Aguirre, Erin Miller, Roger Ford, Oles Andriychuk, Angela Daly and participants of the University of Chicago Junior Scholars Colloquium, the University of Chicago Legal Scholarship Workshop, the University of Strathclyde Law School Centre for Internet Law and Policy Workshop, the 16th Annual Conference of the Italian Association of Law and Economics and of the University of Sao Paulo Antitrust Law and Digital Technology Workshop for insightful comments and discussions.

DISSERTATION DEFENSE COMMITTEE

This dissertation was successfully defended on 18 May 2021 before a committee composed of:

Prof. Lior J. Strahilevitz (Dissertation Supervisor)

Sidley Austin Professor of Law at the University of Chicago Law School

Prof. Luigi Zingales

Robert C. McCormack Distinguished Service Professor of Entrepreneurship and Finance at the University of Chicago Booth School of Business

Prof. Omri Ben-Shahar

Leo and Eileen Herzel Professor of Law at the University of Chicago Law School

Prof. Randal C. Picker (Dissertation Supervisor)

James Parker Hall Distinguished Service Professor of Law at the University of Chicago Law School

Prof. Tom Ginsburg

Leo Spitz Professor of International Law at the University of Chicago Law School

ABSTRACT

This dissertation addresses a number of issues in the regulation of digital markets by means of three different essays.

The first essay studies the political economy of antitrust enforcement across the Atlantic. Many believe that the EU's enforcement actions against US companies are a form of digital protectionism. This essay looks at the foundations of data protection and antitrust policies to propose an alternative explanation. Europeans associate data protection with inalienable rights, Americans treat data as an asset. Europeans use competition policy to advance personal freedom, US antitrust policy focuses on economic efficiency. The combination of these singular EU traits encourages the regulation of internet companies. However, as the US does not share either trait, the EU/US divide over internet regulation will grow. The essay concludes by arguing for an adjusted role for economic reasoning in antitrust enforcement as an avenue to bridge differences.

The second essay addresses the definition of antitrust relevant markets by discussing the American Supreme Court decision in Ohio v. American Express. In a controversial landmark ruling, both the Court's majority and minority battled over definitions of relevant markets in the complex industry of electronic payments: the majority affirmed that "transaction platforms" always constitute a single "two-sided relevant market" and the minority argued that electronic payments are regular complementary goods subject to traditional "one-sided" analysis. This essay challenges both views and proposes a novel multi-layered approach. It then discusses the rich international experience of the EU and Brazil in the application of competition law to of electronic payments' markets as examples of cases where authorities sometimes correctly applied and sometimes fell short of this

multi-layered view. Building on these insights, the essay develops a framework to define relevant markets in cases involving transaction platforms and concludes by outlining the applicability of this layered approach to a variety of markets commonly found in today's digital economy.

The rise of data privacy laws is one of the most profound legal changes of this century. Yet, available data indicates that these laws recurrently suffer from an enforcement gap. This raises the question of the third essay: what accounts for this gap and what can be done to improve the performance of these laws? The essay first describes three core building blocks of data protection regimes in the United States and Europe—namely, market forces, tort liability and regulatory enforcement—that these jurisdictions combine to ensure that companies act in accordance consumers' privacy preferences. It then identifies two key reasons—particularly deep information asymmetries between companies and consumers/regulators, and high levels of market power in many data markets—that enable companies to behave strategically and undermine legal compliance. The conclusion looks at the institutional design of antitrust and anti-fraud laws to argue that an effective online privacy regulatory system should reflect three key principles. First, the system must multiply monitoring and enforcement resources; second, the system must bring violations to light; and third, the system must promote governmental accountability.

Essay 1:
Digital Protectionism? Antitrust, Data Protection and the EU/US Transatlantic Rift*

INTRODUCTION

In 2015, President Obama stated that Europeans were using privacy protection laws as pure digital protectionism.[1] In doing so he echoed American concerns that selective antitrust[2-3] enforcement combined with changes in privacy protection to enable the creation of the European Single Digital Market aimed at harming American business and boosting European players.[4]

---

* This article was originally published in the Journal of Antitrust Enforcement, Volume 7, Issue 1, Pages 27-53 (2019). It is reprinted in this Dissertation in accordance with the Oxford University Press Journals Copyright Policy.

[1] Liz Gannes, 'Obama Says Europe's Aggressiveness Toward Google Comes From Protecting Lesser Competitors' (*Re/code*, 14 February 2015) https://www.recode.net/2015/2/13/11559038/obama-says-europes-aggressiveness-towards-google-comes-from

[2] Anu Bradford, Robert Jackson and Jonathon Zytnick, 'Is EU Merger Control Used for Protectionism? An Empirical Analysis' (2018) 15 Journal for Empirical Legal Studies 165 at166.

[3] The term "antitrust" here is used in its American conception, encompassing all areas of competition policy.

[4] For example, A US Senator accused Europe of using antitrust cases against US tech companies as "nationalistic policies", Jemima Kiss, 'US Senator Accuses Europe of Using Antitrust Cases to Disguise Tech Interests' *The Guardian* (Las Vegas, 8 January 2016) 1. The Financial times described how US companies are under attacked in Europe in "*data protection and competition policy*". Rochelle Toplensky, Duncan Robinson and Madhumita Murgia, 'Facebook Faces More Hurdles after Europe Fine' *The Financial Times* (Brussels and London, 18 May 2017) 1. See also Mark Scott, 'Tech Firms See Protectionism in E.U. Plan to Unify Market' *New York Times* (14 September 2016) B1.

Europeans dismissed Obama's claims of political motivation.[5] However, at least under Americans' eyes, these claims are not completely groundless. US internet companies are under significantly higher regulatory pressure in Europe than at home, leading the Wall Street Journal to call the European Commissioner to Competition their "*nemesis*" and "*de facto global regulator*"[6] and the New York Times to affirm that she "*strikes fear into silicon valley*".[7] European actions that directly impact US companies include antitrust and data protection investigations, record fines and new laws and regulations.[8] Claims of digital protectionism constantly surface whenever a new movement takes place.[9] What is undisputable is that over the past years the gulf between the US' and the EU's approach to antitrust and data protection has been widening, all while businesses and regulators are claiming the need for regulatory harmonization in data markets.[10] It is not clear, however, how and if integration can happen.

---

[5] See Members of the European Parliament, 'Statement on "Digital Protectionism"' http://www.marietjeschaake.eu/wp-content/uploads/2015/09/2015-09-22-MEPs-Statement-on-Digital-Protectionism.pdf

[6] See Sam Schechner and Natalia Drozdiak, 'US Tech Giants Meet Their Nemesis' *Wall Street Journal* (4 April 2018) 1.

[7] Sarah Lyall, 'Who Strikes Fear Into Silicon Valley? Margrethe Vestager, Europe's Antitrust Enforcer' *The New York Times* (6 May 2018) 1.

[8] Such as two antitrust investigations against Google and Facebook, the introduction of an overarching data protection regulation and even changes to national antitrust laws, as will be better explored below.

[9] See, for example, Politico's coverage of the record Google fine, saying "*The case is bound to stoke tensions between Brussels and Washington, where some politicians view the Commission's antitrust enforcement as thinly-veiled protectionism.*". Nicholas Hirst, 'EU's Vestager Hits Google with €2.42 Billion Fine' *POLITICO* (27 June 2017) https://www.politico.eu/article/vestager-hits-google-with-e2-42-billion-fine/

[10] See statements by Commissioners Terrell McSweeny, 'Big Data: Individual Rights and Smart Enforcement - Remarks of Commissioner Terrell McSweeny' https://www.ftc.gov/public-statements/2016/09/big-data-individual-rights-smart-enforcement at 2. and Margrethe Vestager: *"[I]t's not enough for competition authorities to work well in isolation. We also need to work together. (…) As companies go global, so must competition enforcers.*" Margrethe Vestager, 'Competition for a Fairer Society' (*European Commission - European Commission*, 20 September 2016) http://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-fairer-society_en

This paper examines this growing divide under a new framework that integrates public policies on data protection and antitrust. First, it adds a new perspective to the debate by arguing that deep-rooted differences in the historical evolution of both data protection and antitrust policies are a good justification to why the transatlantic gulf is widening. Second it suggests that while harmonization is unlikely (and may be unnecessary), a window of opportunity for international convergence may arise from the renewed EU's focus on private damages in antitrust litigation. It also provides a tentative framework under which this convergence process may take place.

The paper is divided in four parts, other than this introduction. Part one outlines how data protection and antitrust enforcement policies differ across the EU and the US. On the privacy side, while Europeans qualify personal privacy and control over data as an inalienable right, Americans treat it as an asset that may be freely traded. On the antitrust side, Europeans use competition policy as a way to advance personal freedom, allowing fairness and liberty considerations that find no grounds in the US' more efficiency-driven economic-centered approach.

The next two sections are the core of the paper. The second sheds light on the under-explored dynamics that exist between privacy protection and competition policies in data-intensive markets. It shows how a holistic view of antitrust enforcement in data markets that considers the key differences between privacy protection and competition policies across the Atlantic puts the EU in a singular position to push for a formal and informal interconnection between these policies. Compared to the US, European officials have both stronger political motivation and unique tools to regulate internet companies. Therefore, the more the digital economy grows in importance, the more Europe and the US will drift apart, increasing transatlantic tensions. This difference in motivation and tools should prove more salient when traditional antitrust policy does not provide bright-clear answers (grey enforcement zones), such as in many dominance investigations. Indeed,

the so-far best examples of the transatlantic rift involve dominance investigations against Google and Facebook.

Finally, the third discusses how a failure to recognize these differences may lead Americans to misconstrue European actions as mere economic protectionism. However, the framework proposed herein indicates that these actions reflect legitimate distinctive assumptions on what is the role of privacy protection and antitrust policies in a society and, by consequence, how governments should monitor and regulate online markets. Both sides have to gain by recognizing the importance of these cultural differences. Americans must acknowledge them if they are to effectively influence EU policy-making. Europeans must better explain their decisions, lest seeing their actions condemned as arbitrary. The section then argues that both sides can learn from one another when designing an optimal policy for antitrust analysis for data markets and that institutional shifts in the EU may provide a credible opening a window for some harmonization. It also briefly discusses the value of data interoperability tools in minimizing some concerns. Part four is a brief conclusion.

I. THE EU/US DIVIDE IN DATA PROTECTION AND ANTITRUST POLICIES

i. The data protection divide

Privacy is an amorphous concept with different meanings across societies. The EU and the US developed two different cultures of privacy protection[11] that led to different public policies aimed at safeguarding these privacy interests. Currently, Europeans provide more comprehensive

[11] See James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 The Yale Law Journal 1151. p. 1161.

protections to personal privacy in private-private relations than Americans.[12] This section provides an outline of these differences and how they translate into data protection rules.[13] This outline focuses on EU proto-federal and US federal policies as the most important in each jurisdiction, notwithstanding the variations that exist within EU Member-States and US States.[14]

European privacy protection policies reflect much of the French and German cultures of privacy protection as a safeguard of personal honor. Historically, high-status citizens used civil lawsuits to prevent the dissemination of false/negative news that resulted from the expansion of a free press. These lawsuits helped defend personal lives and family honor from lies, insults or unpleasant news while ensuring a private space for deliberation and a right to information self-determination.[15] Under such view, the primary enemy of one's privacy would be private third-parties (the media), capable of publishing false or unpleasant information about someone.[16]

This broad personal privacy right is enshrined on Article 7 of the European Charter of Fundamental Rights, which affirms that '*Everyone has the right to respect for his or her private and family life, home and communications*'.[17] With time, Europeans expanded this right to also

[12] Paul M Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 Harvard Law Review 1966. p. 1176; Lior Strahilevitz, 'Toward a Positive Theory of Privacy Law' (2013) 126 Harvard Law Review 2010. p. 2036-2037.
[13] See also Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 The Georgetown Law Journal 115.
[14] In doing so, this paper follows others such as ibid. and Anu Bradford, 'The Brussels Effect' (2012) 107 Nw. UL Rev. 1 at15-16, 23
[15] Whitman (n 11). p. 1171-1189.
[16] ibid. p. 1160-1162. The European view is similar to the exposed by Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard law review 193. but that found limitations in the US due to conflicts with other constitutionally protected rights, such as freedom of speech.
[17] It is also affirmed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms from 1950, with a similar text.

include data protection, first through a 1981 Convention,[18] then a 1995 Directive,[19] Article 8 of the EU Charter on Fundamental Rights and finally through the new EU-wide General Data Protection Regulation ("GDPR").[20] All these affirmed a regulatory framework that strongly protects EU citizens' fundamental rights in data processing and control by connecting these citizens with EU institutions developed to safeguard these interests. EU data markets are effectively overseen by public agencies, which are allowed impose limits on how parties may obtain, process, publish, transfer or retain data.[21]

This state-intermediated system for data collection and processing is increasingly different from the one in the US. While in the EU online users can be considered "data subjects", in the US they are "online consumers".[22] The American concept of privacy is based on its underlying values of liberty, self-government, self-determination, freedom of expression and the marketplace of ideas. Under this view, the main threat to someone's liberties (and privacy) are not private parties

[18] Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.
[19] The EUR-Lex - 31995L0046 - Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data 1995 (Official Journal L 281 , 23/11/1995 P 0031 - 0050;). Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' [2014] Columbia Law Review 583. P 592-593. Schwartz (n 12). p. 1969-1971.
[20] Regulation 2016/679 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 2016 (OJ L 119, 452016, p 1–88).
[21] Landmark cases include *Case C-101/01 - Criminal Procedure Against Bodil Lindqvist* [2003] CJEU ECLI:EU:C:2003:596; *Case C-73/07 - Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] CJEU - Grand Chamber ECLI:EU:C:2008:727; *Case C-203/15 - Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] CJEU - Grand Chamber ECLI:EU:C:2016:970; *Application 931/13 - Case of Satakunnan Markkinapörssi oy and Satamedia oy v Finland* (European Court of Human Rights - Grand Chamber). *Case C-362/14 - Maximilian Schrems v Data Protection Commissioner* [2015] CJEU ECLI:EU:C:2015:650., *Case C-131/12 - Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] CJEU (Grand Chamber) ECLI:EU:C:2014:317.
[22] Schwartz and Peifer (n 13)., p. 121-123.

(the market or the press), but rather abuse of power by governmental authorities.[23] Americans feared that the growing governmental investigation and repression apparatus would be used to destroy hard-earned civil liberties.[24] The protection of privacy then meant safeguarding a sphere of private deliberation.[25] With time it expanded to also prevent the Government from blocking the dissemination of newsworthy content by newspapers and the media.[26]

This focus on protections against the Government shapes American data protection policies.[27] Except for certain industries and specific uses (e.g. health care, credit reporting), companies are free to contract around data collection, processing and retention.[28] Personal data is as an asset that can be freely traded in private transactions (freely alienable right), subject only to limitations typically applicable to other private contracts (e.g. severe information asymmetry between consumers and companies).[29]

The contrasts between the EU and the US are well exemplified by an analysis of the powers given to data protection regulators. The FTC has no specific data protection mandate nor fining

[23] Whitman (n 11). p. 1211-1216
[24] Richard Alan Clarke and others, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (Office of the Director of National Intelligence 2013).p. 57-8;64
[25] *Olmstead v United States* (1928) 277 SCt 438 (Supreme Court)., p 478 (Brandeis, J., dissenting). *Katz v United States* (1967) 389 SCt 347 (Supreme Court).This may include, for example, one's phone (*Riley v California* (2014) 134 Ct 2473 (Supreme Court).) or the use of GPS to track car movements (*US v Jones* (2012) 132 Ct 945 (Supreme Court).)
[26] See Daniel J Solove and Paul Schwartz, *Information Privacy Law* (6th Edition, Wolters Kluwer 2018)., Chapter 3, quoting, among others, *Cox Broadcasting Corp v Cohn* (1975) 420 SCt 469 (Supreme Court); *Florida Star v BJF* (1989) 491 SCt 524 (Supreme Court).
[27] For example, the Privacy Act 1974 (5 USC 552a). only addresses governmental collection and retention of data.
[28] Solove and Hartzog (n 19). P. 587. Schwartz (n 12). p. 1975.
[29] Omri Ben-Shahar and Lior Jacob Strahilevitz, 'Contracting over Privacy: Introduction' (2016) 45 The Journal of Legal Studies S1. p. S6

authority[30] – it became a regulator after settlements involving consumer rights' violation regarding data collection forced (or allowed) it to use common law to step-in and fill the power vacuum.[31] Rather than trying to impose limits on what companies and consumers may agree on, the FTC regulates private information markets under '*a system of informed consent*', where it ensures that consumers have access to the terms of the transaction to make an informed decision.[32]

Diversely, Article 8 of the EU Charter of Fundamental Rights[33] requires the establishment of independent data protection authorities that impose limits on data collection, processing transfer and use. The GDPR will further strengthen these authorities by giving them a broader mandate and the power to fine companies up to 4% of their annual global turnover.[34]

As a final note, one must stress that these comparisons do not imply the necessary prevalence of one system. While US law may be less data protective, this free-market approach

[30] Strahilevitz (n 12). p 2036. Under Section 5 the FTC does not have the power to fine companies, and most of the enforcement action is through fear of public exposure and threats of a costly litigation.

[31] David A Hyman and William E Kovacic, 'Why Who Does What Matters: Governmental Design and Agency Performance' (2013) 82 Geo. Wash. L. Rev. 1446. P. 18-19; 51-52. Solove and Hartzog (n 19). P. 585. The FTC focuses on '*unfair or deceptive acts or practices in or affecting commerce*'. Section 5 Federal Trade Commission Act 1914 (15 USC §§ 41-58, as amended)., see also Solove and Hartzog (n 19). P. 598-606.

[32] Federal Trade Commission, 'Privacy Online: Fair Information Practices in the Electronic Marketplace - A Report to Congress' https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission. Solove and Hartzog (n 19). P. 592 Federal Trade Commission, 'FTC Policy Statement on Unfairness' https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

[33] It affirms that: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.*"

[34] Article 83(5) of the GDPR. This brings privacy protection closer to antitrust policies in terms of regulatory policy.

may be one of the foundations of US Internet dominance.[35] What one must acknowledge, however, is the important differences in data protection policies across the Atlantic and how they shape regulators incentives to act – as will be seen in more detail below.

ii. The antitrust enforcement divide

As in the privacy part, this section provides a brief outline of the foundations and the differences between the EU proto-federal and the US federal antitrust policies (notwithstanding possible differences at EU Member-State and US State level). While this is a necessary simplification, it emphasizes key differences between the policies across the Atlantic.

US antitrust policy reflects in many ways the rise of the Chicago School in the 1970's, which changed antitrust enforcers' focus from *power* to *incentives*. By using rigorous microeconomic analyses, the school defended that rational firms cannot obtain or enhance monopoly power by means of unilateral action, lest trading profits for pure market-share.[36] A more conservative judiciary mostly accepted these views,[37] leading the US Supreme Court to reverse many of the *per se* approaches to unilateral conducts.[38] Modern US antitrust policy, however, combines the same price theory foundations with game theory and other methodologies to limit these pro-markets views by stressing how conducts can either enhance or diminish consumer

[35] See, in general, Anupam Chander, 'How Law Made Silicon Valley' (2013) 63 Emory Law Review 639. and Solove and Hartzog (n 19). P 591-592, on why the internet industry greatly favors de-regulation.
[36] Richard A Posner, 'The Chicago School of Antitrust Analysis' (1979) 127 University of Pennsylvania Law Review 925. p. 928.
[37] Michael D Whinston, *Lectures on Antitrust Economics* (MIT Press Books 2008). P. 6.
[38] See the Supreme Court decisions in *Continental TV, Inc v GTE Sylvania Inc* (1977) 433 SCt 36 (Supreme Court)., *State Oil Co v Khan* (1997) 522 SCt 3 (Supreme Court). and *Leegin Creative Leather Products v PSKS, Inc* (2007) 127 SCt 2705 (Supreme Court). and a somewhat victory in *Jefferson Parish Hospital Dist No 2 v Hyde* (1984) 466 SCt 2 (Supreme Court).

welfare.[39] Through strong formal economic reasoning, it tries to estimate, albeit imperfectly, the general and consumer welfare impacts of conducts and mergers - increasing the importance of economic experts vis-à-vis that of lawyers. It also emphasizes dynamic competition as the main driver of increases in consumer welfare. All in all, the US analyzes unilateral conducts under a mostly rule of reason approach, in which plaintiffs (including the Government) have a high burden to meet when bringing Section 2 claims against dominant companies.

The European antitrust policy diverges from the American in many ways. It still reflects (at least partially) some of the beliefs of German Ordoliberalism,[40] a concept that helped shape Germany´s economic and political order after the second world war.[41] Under such view, competition has both an important economic and political dimension, as competition deprives companies of economic and associated political power.[42] It affirms a strong State role in keeping markets open to competition (punishing abusive conduct) or, if that is unfeasible or has failed,

[39] Herbert Hovenkamp, *The Antitrust Enterprise: Principle and Execution* (Harvard University Press 2009). p. 38-39. Jorge Padilla and David S Evans, 'Designing Antitrust Rules for Assessing Unilateral Practices: A Neo-Chicago Approach' (2005) 72 University of Chicago Law Review. p. 74 Einer Elhauge, 'Tying, Bundled Discounts, and the Death of the Single Monopoly Profit Theory' (2009) 123 Harvard Law Review 397. P. 400.

[40] Christian Ahlborn and Carsten Grave, 'Walter Eucken and Ordoliberalism: An Introduction from a Consumer Welfare Perspective' (2006) 2 Competition Policy International. p. 199/200. John Vickers, 'Abuse of Market Power' (2005) 115 The Economic Journal F244. P. F246/247. Silvia Beltrametti, 'Capturing the Transplant: US Antitrust Law in the European Union.' (2015) 48 Vanderbilt Journal of Transnational Law. P. 1173-1178; Paul Behrens, 'The Consumer Choice Paradigm in German Ordoliberalism and Its Impact upon EU Competition Law' (2014) Discussion Paper 01/14 Europa-Kolleg Hamburg. p. 24-26.

[41] Ahlborn and Grave (n 40). p. 199/200. Vickers (n 40). P. F246/247. Beltrametti (n 40). P. 1173-1178; Behrens (n 40). p. 24-26. Some challenge how decisively was the ordoliberal influence in EU Competition policy, see Pablo Ibáñez Colomo, 'Beyond the "More Economics-Based Approach": A Legal Perspective on Article 102 TFEU Case Law' (2016) 53 Common Market Law Review 709 at4. While it is not the goal of this paper to settle this debate, one has to point-out that the ordoliberal framework seem to fit well with the current status of EU Competition Law regarding dominant firms, reason why it is mentioned herein.

[42] Ahlborn and Grave (n 40). p. 200/201. Beltrametti (n 40). p. 1176-1178.

taking decisive action to regulate dominant companies, forcing them to behave as if competition was present.[43] This important political connotation further empowers antitrust regulators to take action as a pre-condition to ensuring a fair and democratic society.

For the purposes of this paper, EU antitrust enforcement diverges from the US in at least five important manners:[44] (i) relatively lower thresholds for the characterization of dominance; (i) a view that dominant firms have '*special responsibilities*' towards the market; (iii) a more legalistic approach to unilateral behavior; (iv) the prohibition of exploitative abuses and (v) the growing importance placed on freedom of choice as a theory of harm.

More specifically, US courts require firms to maintain somewhat stable market-shares of at least 70-75% to affirm dominance.[45] Market shares below 50% usually trigger a de facto exemption of antitrust liability.[46] EU case law acknowledges a rebuttable presumption of dominance in case of market-shares above 50%[47] and the Court of Justice of the European Union (CJEU) has affirmed dominance in shares as low as 40%.[48]

---

[43] Ahlborn and Grave (n 40). p. 199-202 and 204-205.

[44] There is another important debate about consumer versus total welfare, though it impacts less directly this discussion. See, Roger D Blair and D Daniel Sokol, 'Welfare Standards in US and EU Antitrust Enforcement' (2012) 81 Fordham L. Rev. 2497.

[45] ABA Section of Antitrust Law, *Antitrust Law Developments* (Eighth, American Bar Association 2017). pgs. 229-232. See also *United States v Aluminum Co of America* (1945) 148 F.2d 416 (2nd Circuit). *United States v EI du Pont de Nemours & Co* (1956) 351 SCt 377 (Supreme Court); *Spirit Airlines, Inc v Northwest Airlines, Inc* (2005) 431 F.3d 917 (6th Circuit); *Conwood Co, LP v US Tobacco Co* (2002) 290 F.3d 768 (6th Circuit).

[46] ABA Section of Antitrust Law (n 45) at231-232, quoting *Bailey v Allgas, Inc* (2002) 284 F.3d 1237 (11th Circuit); *AD/SAT, Div of Skylight, Inc v Associated Press* (1999) 181 F.3d 216 (2nd Circuit); *United Air Lines, Inc v Austin Travel Corp* (1989) 867 F.2d 737 (2nd Circuit).

[47] Ahlborn and Grave (n 40). P. 207. Daniel J Gifford and Robert T Kurdle, *The Atlantic Divide in Antitrust: An Examination of US and EU Competition Policy* (University of Chicago Press 2015). p. 10-11. See also *Case C-62/86 - AKZO v Commission* [1991] CJEU ECLI:EU:C:1991:286. para. 60.

[48] *Case C-95/04 - British Airways v Commission* [2007] CJEU ECLI:EU:C:2007:166, 2007 2331.

Moreover, CJEU case law has also affirmed that dominant firms have '*a special responsibility not to allow its conduct to impair undistorted competition on the common market'*.[49] While the economic justifications and the exact legal contours of this concept are not clear, it generally means that firms with significant market-power (a quasi-monopoly) have a positive obligation to behave as if they did not have such power, adopting special precautions to prevent the emergence of new competition.[50] It also means that while in the US an antitrust violation requires a causal link between the conduct assessed and the firm's market power, in the EU '*a conduct can be abusive even if it does not maintain or strengthen that [market] power*'.[51]

The EU also has a more formalistic approach to many forms of unilateral behavior such as exclusive agreements, price discrimination, tying, bundling and loyalty rebate.[52] EU Courts accepted a presumed harm to competition as a likely result of a conduct,[53] exempting the European Commission from having to prove actual loss of consumer welfare.[54] Europe also condemns

---

[49] See *Case C-322/81 - Michelin/Commission (Michelin I)* [1983] CJEU ECLI:EU:C:1983:313, 1983 3461. para. 57, and *Case C-280/08 P - Deutsche Telekom v Commission* [2010] CJEU ECLI:EU:C:2010:603. para. 176. *Case C-413/14 P - Intel Corporation Inc vs the European Commission* [2017] CJEU ECLI:EU:C:2017:632. para 135.

[50] Robert O'Donoghue and Jorge Padilla, *The Law and Economics of Article 102 TFEU* (2nd edn, Hart Publishing 2013). p. 206-208. Ahlborn and Grave (n 40). p. 208. See *Case C-280/08 P - Deutsche Telekom v. Commission* (n 49). at 125/126.

[51] Vickers (n 40). P. F247

[52] Ahlborn and Grave (n 40). p. 208. Vickers (n 40). p. F248-F253. Gifford and Kurdle (n 47). p. 14-17; 36. Patrick F Todd, 'Out of the Box: Illegal Tying and Google's Suite of Apps for the Android OS' (2017) 13 European Competition Journal 1 at 69-75.

[53] Christian Ahlborn and David S Evans, 'The Microsoft Judgment and Its Implications for Competition Policy towards Dominant Firms in Europe' (2009) 75 Antitrust Law Journal 887. p. 902. and Francisco Marcos, 'The Prohibition of Single-Firm Market Abuses: US Monopolization versus EU Abuse of Dominance' [2017] International Company and Commercial Law Review. p. 8.

[54] O'Donoghue and Padilla (n 50). p. 269-270. *Case T-203/01 - Michelin v Commission (Michelin II)* [2003] CFI ECLI:EU:T:2003:250, 2003 4071; *Case C-95/04 - British Airways v. Commission* (n 48); *88/138/EEC - Eurofix-Bauco v Hilti* (1988) 1988 19 (European Commission); *Case 85/76 - Hoffmann-La Roche v Commission* [1979] CJEU ECLI:EU:C:1979:36, 1979 461; *Case T-65/98 - Van den Bergh Foods v Commission* [2003] CFI

exploitative practices,[55] allowing the use of antitrust laws to proscribe the charging excessive prices that lead to direct loss of consumer welfare (unfair prices or rent extraction).[56] In the US, lawfully acquired monopolies are free to charge supra-competitive prices, as these prices reward companies for their superior efforts and are what drive competition and economic growth.[57]

Finally, the European Commission and the CJEU are assigning a growing importance to the emerging concept of freedom of choice as a theory of harm.[58] This theory views competition as a dynamic process of discovery between consumers and firms. Concentrated markets deprive consumers of choice between different suppliers and, therefore, denies them an important

---

ECLI:EU:T:2003:281, 2003 4653. and *Case T-201/04, Microsoft vs Commission* [2007] CFI ECLI:EU:T:2007:289. The CJEU decision in *Intel vs. Commission* (n 49). And the potentially larger role played by the "As Efficient Competitor" test complicates this. Nonetheless, the CJEU affirmed the prima facie presumption of harm and the special responsibility of dominant companies in ensuring that their practices do not harm competition (*ibid.* paras.132-140). These presumptions still tilt the playing field in favor of the Commission in findings of infringement.

[55] Article 102(a) TFEU. See also Richard Whish and David Bailey, *Competition Law* (8th edn, Oxford University Press 2015). p. 759-766.

[56] O'Donoghue and Padilla (n 50). p. 732. There are challenges in the prosecution of exploitative abuses (e.g. cost determination, incentives given to firms, comparison across products, etc.), so case law is somewhat limited - but exists (see *Case C-27/76 - United Brands v Commission* [1978] CJEU ECLI:EU:C:1978:22, 1978 207; *Case 26/75 - General Motors Continental NV v Commission* [1975] CJEU ECLI:EU:C:1975:150; *Case 226/84 - British Leyland v Commission* [1986] CJEU ECLI:EU:C:1986:421, 1986 3263.). European authorities are clarifying a methodology which allows them to bring more cases and authorities have vowed to enforce price abuses (See *Case C-177/16 - Biedrība 'Autortiesību Un Komunicēšanās Konsultāciju Aģentūra – Latvijas Autoru Apvienība' v Konkurences Padome* [2017] CJEU ECLI:EU:C:2017:689. and Margrethe Vestager, 'Protecting Consumers from Exploitation' (*European Commission - European Commission*, 21 November 2016) http://ec.europa.eu/commission/2014-2019/vestager/announcements/protecting-consumers-exploitation_en

[57] See *United States v. Aluminum Co. of America* (n 45). and *Verizon Communications Inc v Law Offices of Curtis V Trinko, LLP* (2004) 540 SCt 398 (Supreme Court).

[58] See, generally, Paul Nihoul, Nicolas Charbit and Elisa Ramundo, *Choice - A New Standard for Competition Law Analysis?* (1st edn, Concurrences 2016). Behrens (n 40); Paul Nihoul, 'Freedom of Choice – The Emergence of a Powerful Concept in European Competition Law' (2012) 3 Concurrences Review 55. quoting cases *Case C-202/07 P - France Telecom v Commission* [2009] CJEU ECLI:EU:C:2009:214, 2009 2009; *Case T-201/04, Microsoft vs. Commission* (n 54); *Case C-322/81 - Michelin/Commission (Michelin I)* (n 49).

individual freedom associated with increased rivalry in any given market. A key role of antitrust regulators then becomes to protect consumer welfare by ensuring that consumer choice is not unduly restricted by abusive behavior that excludes competitors from the market – even if a reasonable efficiency justification is present.[59] This approach differs from the US view on dominance violations, where a conduct is reprievable if a dominant company raises rivals' costs without a clear efficiency justification.[60]

II. A FORMAL AND INFORMAL INTERCONNECTION BETWEEN DATA PROTECTION AND ANTITRUST ENFORCEMENT

i. Expanding the core of competition policy to reflect data concerns

Competition policy is not an exact science solely focused on maximizing consumer welfare and applied uniformly across different jurisdictions. Rather, as any other public policy, it reflects a series of political choices made by societies, who can prioritize certain policy goals at the expense of others.[61] Competition agencies are designed to be responsive to political choices. Competition commissioners are appointed by politicians; Congress and other deliberative bodies establish the

[59] Behrens (n 40). p. 27-32.
[60] Andrew I Gavil, William E Kovacic and Jonathan B Baker, *Antitrust Law in Perspective: Cases, Concepts, and Problems in Competition Policy* (Thomson/West 2008). p. 639-640, 666-670.
[61] Ariel Ezrachi, 'Sponge' (2016) 5 Journal of Antitrust Enforcement 49. p. 2, p. 6 David A Hyman and William E Kovacic, 'Institutional Design, Agency Life Cycle, and the Goals of Competition Law' (2012) 81 Fordham L. Rev. 2163. p. 2170-2172. Vestager affirmed: "*The second question is: Does competition enforcement relate to wider political priorities? And does it inform regulatory and other action taken to implement such priorities? Again, the answer is: Yes, it does.*" Margrethe Vestager, 'The Future of Competition' (*European Commission - European Commission*, 2 October 2015) https://ec.europa.eu/commission/2014-2019/vestager/announcements/future-competition_en

legislative goals of competition authorities and allocate budgets depending on how well they see their performance (among others).[62]

By pointing out the above, this paper does not wish to underestimate the general importance of economics to antitrust enforcement. Modern antitrust policy embraces economics: microeconomics and industrial organization play a crucial role in providing uniformity, guidance and stability to competition policy.[63] However, even a "purely economics-based" approach to antitrust policy would lead to divergence as economic results constantly differ.[64] There is no one size fits all standard to competition policies.

Using Ezrachi's analogy, competition policy should be better seen as a sponge that has a political core, an economic membrane and external by-passes. The core is jurisdiction-specific and encompasses both general values on the maximization of consumer welfare and national social and political priorities that shape local enforcement.[65] The incorporation of multiple local political priorities may lead to arbitrary and unpredictable enforcement, undermining the legitimacy of competition agencies.[66] Thus, the second layer is an economic membrane that exerts external pressure on the political core.[67] Economics provides a *lingua-franca* to competition authorities

---

[62] Hyman and Kovacic (n 61). p. 2170-2174. William E Kovacic and David A Hyman, 'Competition Agency Design: What's on the Menu?' (2012) 8 European Competition Journal 527. p. 532-533. Examples include Europeans explicitly using antitrust to promote the common market (Alison Jones and Brenda Sufrin, *EU Competition Law: Text, Cases, and Materials* (6th edn, Oxford University Press 2016). p. 35) or the US' Robinson-Patman Act's prohibitions on price discrimination and the State Action and Noerr-Pennington doctrines.
[63] David S Evans, 'Why Different Jurisdictions Do Not (and Should Not) Adopt the Same Antitrust Rules' (2009) 10 Chi. J. Int'l L. 161. P. 167.
[64] ibid. p. 162. Simon Bishop, 'Snake-Oil With Mathematics Is Still Snakeoil: Why Recent Trends in the Application of So-Called "Sophisticated" Economics Is Hindering Good Competition Policy Enforcement' (2013) 9 European Competition Journal 67. p. 68-69.
[65] Ezrachi (n 61). p. 4-14.
[66] Hyman and Kovacic (n 61). p. 2170.
[67] Ezrachi (n 61). p. 17.

through a homogeneous rationale and benchmark that prevents excessive expansion of competition policy, increases predictability and facilitates convergence. Finally, there are explicit external political by-passes – clear political choices that favor other social priorities over the enforcement of "welfare maximizing" competition policy.[68]

This political core is where the EU/US divide on data protection helps explain part of the conflicts taking place between both jurisdictions. As seen above, Europeans are wary of private (and public) institutions amassing personal data, leading the EU as a community to codify a fundamental right to data protection that empowers institutions to oversee the gathering, processing and using of personal information.[69]

Antitrust policies should reflect the changes taking place at various levels of European policymaking, as regulators adapt enforcement to the priorities of Europe as a society. This translates into the EU having both the *political motivation* and the *necessary toolkit* to push for both the *formal* and *informal* integration between privacy and competition policy. Formal integration takes place whenever antitrust policies are explicitly used to address data protection issues – as the German Facebook case below demonstrates. Informal integration may take place whenever concerns about the power of data companies generally encourages regulators to take action against such firms (even if not necessarily data related) as a way to rein-in their economic power – with the Google case also described below as another potentially good example. The

[68] ibid. p. 22-25. Examples again are the State Action and Noerr-Pennington Doctrines in the US or EU specific insurance block exemptions and rules for agricultural products.

[69] This is also a strategic view, as with the creation of EU Digital Single Market, Europeans have an express goal of becoming '*a hub for data services which require both free flows and trust*'. See European Commission, 'Exchanging and Protecting Personal Data in a Globalised World - COM(2017) 7' http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN at 3

interconnection of both policies should create an "amplifying effect" that will drift Europe further away from the US, exacerbating transatlantic tensions.

One has to note that this "political motivation" does not imply that all enforcement action against data companies is politically motivated, something that would equate protectionism. On the contrary, what this paper defends is that Europe as a jurisdiction has developed a legal framework that encourages the strong regulation of data markets as a way to protect fundamental rights. Part of this may come through antitrust regulators' taking action against the economic power of data companies.

There are important links between antitrust and data protection, leading to a growing debate in academia,[70] the general press,[71] and case law[72] on the role of data as key asset in information markets. By regulating a key input, data protection policies shape data markets.[73] Limits on data gathering, processing and use established by regulations outline the framework in which companies operate, develop new products and compete to attract demand, among others. In addition, data feedback loops may easily entrench market-power by increasing barriers to entry

[70] See, generally, Maurice Stucke and Allen Grunes, *Big Data and Competition Policy* (1st edn, Oxford University Press 2016).
[71] See 'The World's Most Valuable Resource - Data and the New Rules of Competition' [2017] *The Economist* http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource
[72] See the Facebook investigation taking place in Germany or *M8124 - Microsoft LinkedIn* (European Commission) at 34-35.
[73] See, generally, Randal C Picker, 'Competition and Privacy in Web 2.0 and the Cloud' (2008) 103 Northwestern University Law Review Colloquy 1., Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2016) 54 Common Market Law Review 11. and 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' https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

and switching costs, strengthening network effects, economies of scale and scope and others.[74] Antitrust authorities, tasked with assuring the proper functioning of markets, will ultimately address what role the access to and control of user data plays in these markets. In doing so, they will also consider how effective are antitrust remedies in addressing data concerns.[75]

This is better seen as a regulator's endogenous decision that reflects both the political climate in which he operates and the toolkit at his disposal - leading different regulators to opt for different solutions. As a result, it is feasible that European antitrust policymakers' actions partially reflect concerns regarding the economic power of companies that handle large amounts of personal data. In the US, the response may be different, as local preferences and available tools are different. In other words, if agencies are '*continually engaged in a process of accumulating and spending political capital*' when taking enforcement decisions,[76] European regulators have incentives to increasingly take action to reign-in, through all means available (antitrust being an important one),

[74] See the Bundeskartellamt preliminary opinion that Facebook is abusing its dominant position, where it affirms that control over data strengthens both direct and indirect network effects, increases barriers to entry and contributes to customer lock-in. Bundeskartellamt, 'Background Information on the Facebook Proceeding' http://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.html?nn=3600108 at 3. or Picker (n 73) at 6-8.

[75] This may not lead to a coherent framework in data protection. In many cases, the weakening of a data company's economic power requires the sharing of such data – something that violate privacy interests. This leads to an inherent tension between data protection and antitrust and, generally, antitrust remedies are ill-equipped to address data protection concerns. See Maureen K Ohlhausen and Alexander Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 Antitrust Law Journal 121., p 155. In order to scape this tension, some regulators such as the EDPS have favored creating a digital clearing house to coordinate the regulation of data markets in the EU. See European Data Protection Supervisor, 'Opinion 08/2016 - EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data' <https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf>. The suggested coordination, however, requires consumers starting to value more privacy. Unfortunately, current behavior suggests that consumers still prefer the added benefits of data aggregation and free services, as shown by DuckDuckGo's market-share of 0.2% in the US.

[76] Hyman and Kovacic (n 31). p. 25

on the power of data companies. In doing so, they demonstrate their alignment to political priorities and *accumulate* political capital to spend in other areas. The same does not hold true for American regulators operating in a political environment where similar actions entail an expenditure of political capital that may be better allocated elsewhere.[77]

This claim should be made with a necessary caveat that it is valid in fringe cases – that is, cases located in the "*grey area*" where traditional economic analysis does not provide a clear answer. As mentioned in the beginning of this section, modern antitrust policies embrace economics – and the EU and the US are at the vanguard. Whenever these authorities are faced with situations where one can identify clear pro or anticompetitive effects, it is expected that they adopt similar decisions – even in cases touching on control of personal data.[78] The framework proposed herein applies then in cases where theories of harm are less clear and economic reasoning can be used to justify enforcement action or acquittal decisions. This is particularly true in dominance investigations (focus of this article), where the practices under scrutiny are usually adopted by other market participants. In such circumstances, findings of violation vis-à-vis legal competition on the merits many times hinge on more subjective concepts such as lack of economic

[77] See the repeal of the privacy protection regulations put in place by the Federal Communications Commission, which led a Financial Times report to declare the U.S. the "*Wild West for Personal Data*". FT Views, 'Digital Privacy Is More than Just Opting in or Out' *Financial Times* (31 March 2017) https://www.ft.com/content/6bb17082-15f1-11e7-80f4-13e067d5072c

[78] This was the case, for example, in the review of merger transactions such as Google/DoubleClick, Microsoft/Yahoo, Facebook/WhatsApp (decided before data protection gained such a prominence in the public debate) or even Microsoft/LinkedIn, where US and EU authorities reached substantively similar conclusions. It was also the case in Bazaarvoice/PowerReviews, a data merger to create a monopoly blocked by the US DoJ, where internal documents pointed out that PowerReview was Bazaarvoice's "*only real competitor*", among other telling evidence (*US v Bazaarvoice, Inc* [2014] ND California No. 3:2013cv00133., p 21).

justification,[79] business strategy rationale and intent to exclude,[80] or presumptions of illegality if the practice is adopted by a dominant company (but legal otherwise).[81] Nonetheless, one can imagine an expansion of this dynamic to other areas where economic reasoning provides less clear results, such as vertical mergers or conglomerate mergers.

The German Facebook and the EU Google dominance investigations exemplify how the combination of political setting and available toolkit lead to different results on the enforcement of competition policies in data markets between the EU and the US. Nonetheless, it is important to acknowledge that this framework aims to anticipate a widening gap in antitrust enforcement, something that limits the number of leading cases that may be presently quoted, though this number may rise quickly.[82]

---

[79] As in *Aspen Skiing Co v Aspen Highlands Skiing Corp* (1985) 472 SCt 585 (Supreme Court).
[80] Even if it is not a requirement for finding of infringement. See, for example, *Case C-549/10P - Tomra Systems and Others v Commission* [2012] CJEU ECLI:EU:C:2012:221., para 19-20. or *Case C-52/09 - Konkurrensverket v TeliaSonera Sverige AB* [2011] CJEU ECLI:EU:C:2011:83. para 88-89.
[81] See, for example, W Kip Viscusi, Joseph E Harrington and John M Vernon, *Economics of Regulation and Antitrust* (MIT press 2005)., p. 294. Francisco E González-Dias and John Temple Lang, 'The Concept of Abuse', *EU Competition Law*, vol Volume V-Abuse of Dominance Under Article 102 TFEU (1st edn, Claeys & Casteels 2013). pgs. 116-122. Hence why European Courts have developed a concept of "special responsibility" in cases such as *Case C-322/81 - Michelin/Commission (Michelin I)* (n 49); *Case C-280/08 P - Deutsche Telekom v. Commission* (n 49); *Case C-12/03 P - Tetra Laval v Commission* [2005] CJEU ECLI:EU:C:2005:87, 2002 4381.
[82] Indeed, Google is already facing two other important antitrust investigations in the EU involving the Android operating system and its AdSense platform. See European Commission, 'Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service - Factsheet' (27 June 2017) http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm and The European Commission has taken the acquisition of Shazam by Apple to Phase II, citing strong concerns in the combination of both companies' databases (European Commission, 'Press Release - Mergers: Commission Opens in-Depth Investigation into Apple's Proposed Acquisition of Shazam' (23 April 2018) http://europa.eu/rapid/press-release_IP-18-3505_en.htm. Other signs also point in the same direction. EU authorities also affirmed that control over data will be subject to scrutiny. In the meanwhile, the FTC affirmed that affirmed that markets have strong incentives to prevent general harm relating to data FTC report on Consumers and Big Data, Federal Trade

ii. The EU toolkit as an incubator for a formal and informal connection between competition and data protection policies

The subsection above discussed how the core of competition policy in the EU may expand to include (legitimate) data protection considerations. This subsection will use the abovementioned Facebook and Google investigations to present how the EU's competition law toolkit should prove a good incubator in which to foster a *formal and an informal* interconnection between data protection and antitrust. That is because Europe's focus on market structure allows authorities to by-pass or apply presumptions to many of the challenges associated with enforcing antitrust in internet markets. As the same by-passes and presumptions are not present in the US, Americans may increasingly misconstrue the actions of their European counterparts as pure digital protectionism.

More specifically, the application of a traditional, economics-based antitrust analysis to multi-sided internet markets faces several hurdles in the definition of relevant markets, assessment of market power and calculation of exclusion, efficiencies and consumer harm.[83] These are in many ways associated with the multi-sided nature of the businesses, the dynamic nature of competition in these markets, as well as the difficulties in defining relevant markets, market power and quantifying consumer harm when services are provided for free. For example, in an antitrust lawsuit against Google for abuse of dominance, the Northern District of California affirmed that

Commission, 'Big Data: A Tool for Inclusion or Exclusion - FTC Report' https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

[83] See, for example, OECD, 'Rethinking Antitrust Tools for Multisided Platforms' http://www.oecd.org/daf/competition/Rethinking-antitrust-tools-for-multi-sided-platforms-2018.pdf , part I or David S Evans and Richard Schmalensee, 'The Antitrust Analysis of Multi-Sided Platform Businesses', *The Oxford Handbook of International Antitrust Economics*, vol 1 (Oxford University Press 2014).

there cannot be any consumer harm when services are provided for free as there is no market for free services that serves the purposes of antitrust laws.[84]

The EU, however, emphasizes static over dynamic competition when defining relevant markets and market power in dominance cases.[85] Therefore, European authorities may define relevant markets in a more conservative manner and presume dominance at shares above 50%. EU authorities also have an easier framework in which to affirm violations of antitrust rules by dominant companies. They may claim that dominant businesses such as Google or Facebook have a special obligation to assure that competition is not impaired by their actions. In addition, the EU's more formalistic approach to unilateral behavior allows the European Commission to presume harm to consumers as the likely result of specific policies adopted by dominant-firms, by-passing the challenges associated with the proper quantification of consumer harm.

Finally, EU authorities may bring forward freedom of choice or exploitative abuses as a theory of harm that justifies antitrust claims against dominant companies. One of the most important defenses available to dominant companies in the US is that they have obtained their monopoly in a lawful way, as a result of their superior product, business acumen or historical accident. European authorities, however, may ignore this line of argument by claiming that dominant companies have an obligation to behave as if they were in a competitive market, despite the path by which they reached their dominant position. In other words, European authorities are capable of going after companies for the pure appropriation of consumer surplus (exploitative abuse) or for the exclusion of competitors that limits consumer choice (freedom of choice theory

[84] *Kinderstart.com LLC v Google Inc* (ND California). p. 4.
[85] Evans (n 63). p. 181.

of harm), something that US regulators may not. Pharmaceutical companies, for example, are being subject to a growing number of exploitative abuse cases both at EU and national level.[86]

These features provide European authorities with a singular toolkit, using antitrust policies to answer concerns regarding the power of internet companies. In some cases, there might be a *formal* interconnection between antitrust and privacy protection policies. This is well exemplified by the preliminary opinion issued by the German antitrust authority[87] affirming that Facebook abused its dominant position by infringing EU data protection rules. In a summary, the Bundeskartellamt affirmed that: (i) Facebook, with a 90% market-share, holds a dominant position in the market for social networks, narrowly defined to exclude services such as Twitter, LinkedIn, WhatsApp or Instagram; (ii) as a dominant company, it is subject to stricter obligations that prevent it from exploiting consumers; and (iii) it has abused this dominant position by imposing exploitative business terms to consumers that violate other laws – in this particular case preventing them from ensuring their fundamental right to information self-determination (collecting more personal data than would be fair).[88]

---

[86] See *Case CE/9742-13 - Unfair pricing in respect of the supply of phenytoin sodium capsules in the UK* (Competition and Markets Authority)., Autorita Garante della Concorrenza e del Mercato, 'A480 - Price Increases for Cancer Drugs up to 1500%: The ICA Imposes a 5 Million Euro Fine on the Multinational Aspen' (14 October 2016) http://www.agcm.it/en/newsroom/press-releases/2339-a480-price-increases-for-cancer-drugs-up-to-1500-the-ica-imposes-a-5-million-euro-fine-on-the-multinational-aspen.html and European Commission, 'Press Release - Antitrust: Commission Opens Formal Investigation into Aspen Pharma's Pricing Practices for Cancer Medicines' (15 May 2017) http://europa.eu/rapid/press-release_IP-17-1323_en.htm

[87] While this is a German case, it is described here both because it can be grounded in European Law (see Giulia Schneider, 'Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's Investigation against Facebook' (2018) 9 Journal of European Competition Law & Practice 213., p. 222-223) and because it may suggest a future path to be followed by the European Commission (Natalia Drozdiak, 'EU Asks: Does Control of "Big Data" Kill Competition?' *Wall Street Journal* (2 January 2018) https://www.wsj.com/articles/eu-competition-chief-tracks-how-companies-use-big-data-1514889000

[88] Bundeskartellamt (n 74). Pgs. 2-4. See also Schneider (n 87). p. 218, 220 and 222.

Such theory of harm would be unacceptable in the US where Facebook would strongly contest market-definition, dominance, any special obligation to protect competition and affirm that, even if it charged supra-competitive prices for their services, these would be lawful given Facebook's superior product.

This easier framework to affirm antitrust violations in internet markets is also exemplified by the evolution of Google's comparison-shopping cases on both sides of the Atlantic. Although the comparison-shopping investigation does not have a direct data protection component, the framework proposed herein demonstrates how general distrust of major data companies empowers the European Commission to take enforcement action against internet companies such as Google[89] – an *informal* connection between antitrust and data protection policies. It is somewhat telling that when considering a "grey case" where a business' conduct could be considered pro-competitive or exclusionary, regulators in the EU and the US reached opposite conclusions.

In short, these cases discussed whether Google illegally benefitted its own comparison-shopping tools by assigning it a prominent place in its search results. The European Commission

[89] Google faced heavy opposition from EU's politicians and commissioners throughout the procedure and they were key in the unprecedented rejection of three commitment proposals. In addition, a key complainant was BEUC, Europe's largest consumer protection association, who hailed the Commission's final decision as a "*game changer*". Part of this intervention is reflecting the fact that less than a quarter of Europeans trust search engines to protect their data, increasing calls for further government action. See Charles Arthur, 'European Commission Reopens Google Antitrust Investigation' *The Guardian* (8 September 2014) http://www.theguardian.com/technology/2014/sep/08/european-commission-reopens-google-antitrust-investigation-after-political-storm-over-proposed-settlement ; BEUC, 'Fair Internet Search - Remedies in the Google Case' http://www.beuc.eu/publications/2013-00211-01-e.pdf ; 'Google Hit with Record $2.7 Billion Fine in EU Antitrust Case' *Reuters* (27 June 2017) http://fortune.com/2017/06/27/google-billion-fine-eu-antitrust-case/ ; European Commission, 'Data Protection Survey' http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/search/data%20protection/surveyKy/2075 at 25.

imposed a record EUR 2.4 billion fine on Google[90] and required the company to develop a "search neutral" system which does not violate EU competition laws – something Google is now trying to implement.[91] In its decision, the European Commission: (i) affirmed that general search services are an economic activity because, even if free, users pay for such services by providing their personal data;[92] (ii) used mostly qualitative data to define narrow relevant markets, general search and comparison shopping search (ruling out competition with merchant websites such as Amazon and eBay);[93] (iii) affirmed that Google is dominant on general search and, as such, had a special responsibility not to harm competition;[94] (iv) concluded that Google has systematically given prominent placement to its own comparison shopping tools and had also demoted comparison shopping services in general search;[95] and (v) concluded that as a result, Google stifled competition by imposing losses on other rivals and depriving consumers of innovation and freedom to choose alterative supplier.[96]

The outcome in Europe was opposite to both a similar FTC investigation (where Google's vertical search practices were cleared) and the KinderStart private lawsuit against Google in Federal Courts, where the Northern District of California ruled out the possibility of antitrust harm arising from practices similar to those that justified Google's European condemnation.

---

[90] See European Commission, 'EC Google Decision - Factsheet' (n 82). And *Case AT 39740 - Google Search (Shopping)* (European Commission).
[91] See Nicholas Hirst, 'Google Submits Search Changes to EU Antitrust Regulators' *POLITICO* (29 August 2017) http://www.politico.eu/article/google-propose-search-changes-to-eu-antitrust-regulators/
[92] *Case AT 39740 - Google Search (Shopping)* (n 90).para. 158.
[93] It also affirmed that Google's practices would have been abusive even if merchant websites were included in the market definition. See *ibid.*, Section 5.2.2.
[94] *ibid.* paras. 271 and 331.
[95] ibid. para. 341.
[96] ibid. Section 7.3.1.

More specifically, after a long investigation, FTC staff affirmed the legality of Google's changes to search results, despite having found direct evidence that (i) Google demoted its rivals in shopping results; (ii) that such demotion could break rival companies; and (iii) that Google was directly using its strong position in search to force potentially competing companies to give-up assets.[97] The FTC apparently overcame the initial hurdles in the definition of relevant markets and in affirming dominance by generally defining a relevant market for general search, a secondary market for *vertical search services* and affirmed Google is '*clearly the dominant provider of 'general search' in the United States*' with a market share of at least 66.7%.[98] However, although it recognized that consumers may be harmed by reduced innovation,[99] the FTC affirmed that: American Courts are skeptical of antitrust harm caused by innovation and new product design features (based on *Microsoft*); since the Supreme Court decision on Trinko, Google would be under no obligation to assist its rivals; and concluded by saying that American Courts have been reluctant to accept Section 2 cases where companies that have been legally trying to protect its market-share end up harming competitors and entrenching its market-power.[100]

---

[97] The Wall Street Journal obtained a leaked confidential memo in which the FTC staffed discussed the Google investigation, see Brody Mullins, Rolfe Winkler and Brent Kendall, 'Inside the U.S. Antitrust Probe of Google' *Wall Street Journal* (19 March 2015) http://www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274 . See, in particular, at 30, Federal Trade Commission, 'FTC Report on Google' http://graphics.wsj.com/google-ftc-report/img/ftc-ocr-watermark.pdf

[98] See Federal Trade Commission, 'FTC Report on Google' (n 97)., pages 60-74. In there, the FTC tries to implement a SSNIP test on the advertising side of the market to help define a relevant market of search advertising and search syndication which it would use to go against Google on the AdSense terms – an investigation also ongoing in Europe. However, and consistent to the exposed herein, the agency apparently ruled out the application of any economic test usually employed in the definition of relevant markets and dominance when making such assessments for the comparison-shopping case.

[99] ibid. at 80.

[100] ibid. at 82-86.

All in all, the experience shows how the US' less deferential legal system effectively prevented the FTC from taking the exact same course of action the European Commission adopted in Europe, where a more legalistic framework reduces the role played by European Courts in reviewing dominance condemnations.

The FTC's reluctance in bringing a claim appears justified when one looks at the KinderStart litigation against Google – an attempt by a private party to appeal directly to Courts (by-passing the FTC). KinderStart, a vertical search website for kids' products and services, filed a private claim against Google for attempted monopolization and monopolization of markets in violation of Section 2 of the Sherman Act – similar to the EU decision against Google. The claim was that Google manipulated its page rank algorithm to voluntarily demote KinderStart's search rank. This decreased KinderStart's website traffic and led to losses in both commercial and advertisement revenue. Among others, KinderStart also alleged that Google charged exorbitant prices for its ad placement services because of its market power.

The lawsuit, however, was summarily dismissed by the Federal Court of the Northern District of California. In his opinion granting Google's motion to dismiss without leave to amend, Judge Fogel affirmed that: (i) the search market was not a relevant market for the purposes of antitrust laws because users or companies do not pay to be listed on general search results;[101] (ii) Google would have no specific intention to monopolize as KinderStart did not prove that it competed with Google;[102] (iii) the Supreme Court's Trinko decision reaffirmed that simply charging high prices is not a violation of antitrust laws;[103] (iv) although KinderStart showed that Google had a market share in excess of 75% in the search market, this alone was not proof that

[101] *Kinderstart v. Google* (n 84) at 4
[102] *ibid.* at5
[103] *ibid.* at7.

Google had market power to violate antitrust laws;[104] (v) that even if KinderStart were removed from the market, this is not an injury that antitrust laws are trying to prevent unless the company can prove that this removal harms consumer welfare;[105] and, finally, that (vi) Google is under no obligation to aid a potential rival and it has no obligation to deal with KinderStart (Google is not an essential facility).[106]

This comparison between the EU and US experiences exemplifies how the European toolkit is well-placed to overcome the challenges faced by antitrust plaintiffs in when filing lawsuits against internet companies in the US.

III. THE WAY AHEAD: CONVERGENCE OR DIVERGENCE?

So far, this paper presented how the differences between the American and European approaches to data protection provide EU regulators with motivation to strengthen antitrust enforcement in data markets. Moreover, it argued that once this process starts, the unique features of European antitrust policy will prove a perfect incubator, so that antitrust cases against US tech companies for dominance violations should grow. Americans do not share and may not understand neither the motivation nor the antitrust tools employed in the EU.[107] As the Atlantic divide on

---

[104] The Court pointed other factors which may also indicate Google's market power, but affirmed that since KinderStart failed to define a relevant market, it did not have to issue an opinion on that matter. *ibid.* at 8.
[105] *ibid.* at 8.
[106] *ibid.* at 9-10. This is also opposite to the EU, were Courts recurrently affirmed obligations to deal if the asset is essential for competition. Marcos (n 53). p. 18-19.
[107] An example is Apple's CEO comparing the EU State-aid rules to Venezuela's "arbitrary" legal system and the Wall Street Journal Editorial Board affirming that these rules risked turning "*the European Union into a banana republic on high-speed rail*". Rochelle Toplensky, 'Margrethe Vestager, the Woman Who Took the Fight to Apple' *Financial Times* (8 December 2016) https://www.ft.com/content/0055d3ea-bc06-11e6-8b45-b8b81dd5d080 . And 'Vestager Gets Vindictive' *Wall Street Journal* (21 September 2016) 1.

antitrust enforcement widens (and given that actual protectionist policies are on the rise)[108] calls of digital protectionism should afloat. Tensions run both ways, as Europeans may also be startled by American complaints against what they see as a regular application of the rule of law.[109]

Increased strains between two of the world's leading trade and security partners can do little good.[110] The digital economy is a sensitive area and the EU/US safe harbor for data transfer is proof of the damage that may arise from disputes. The first Safe Harbor came after a major trade conflict between the EU and the US over personal data.[111] By striking it down, EU Courts' placed thousands of American and European companies in disarray,[112] reason why business leaders in both jurisdictions welcomed the swift conclusion of the Privacy Shield.[113] The challenge remains, however, on whether it is desirable or possible to bridge such significant cultural differences, or at least develop clear mechanisms that prevents tensions arising from pure misunderstanding.

This remains a contingent question. On one side, convergence may never be necessary. It is perfectly reasonable and may even be optimal that different legal systems will provide different

---

[108] International Chamber of Commerce, 'ICC's Open Market Index - 2017' https://iccwbo.org/publication/icc-open-markets-index-2017/

[109] See European Parliament members' response to Obama: "The political debates on the way forward [on privacy protection] are not a 'Transatlantic rift' and should not be made into one. Rather they represent different views and beliefs that run right through our societies. We consider close cooperation between the EU and the US as vital in a changing world. Neither reaction will help smooth international relations between two of the world's leading trading partners" Members of the European Parliament (n 5).

[110] The EU and the US are the world's leading exporters of digital goods, with a surplus of USD 168 Billion and USD 151 Billion (respectively) and respond for the largest cross-border data flows, twice the US/Latin America flows and 50% more than US/Asia flows. Martin A Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield'. p. 4.

[111] Whitman (n 11). p. 1156.

[112] Weiss and Archick (n 110). p. 3.

[113] Information Technology Industry Council, 'Tech Industry Leaders Commend Conclusion of Safe Harbor Transatlantic Data Transfer Negotiations' (2 February 2016) http://www.itic.org/news-events/news-releases/tech-industry-leaders-commend-conclusion-of-safe-harbor-transatlantic-data-transfer-negotiations

solutions to challenges of a new internet era, forcing agents to adapt to the norms of a given jurisdiction.[114] Lack of convergence is burdensome and may increase the cost of doing business across the Atlantic,[115] but the so far successful implementation of the "right to be forgotten" experience in Europe demonstrates that both markets are large enough to justify companies adopting different solutions. The risk is that shifts in market behavior may lead to the "Brussels' effect" and the export of stricter standards,[116] something that may trigger unpredictable reactions by US authorities facing loss of sovereignty.

On the other, the safe harbor demonstrates how convergence is possible if parties move to bridge differences. As there is more to explore from an academic perspective in this second scenario, this section will focus on that. Bringing together such disparate regimes will require both political motivation and a coherent framework. This part argues that: (i) convergence efforts will require a balancing of the role that economics plays in antitrust enforcement on internet markets on both sides of the Atlantic; and (ii) that recent EU reforms open a window of opportunity for this to happen. In addition, it presents data portability as a mitigating measure that companies may explore to decrease tensions while and if converge does not take place.

[114] For a similar point on antitrust, see Evans (n 63).
[115] Weiss and Archick (n 110). p. 15. European Commission, 'Exchanging and Protecting Personal Data in a Globalised World - COM(2017) 7' (n 69). at 2. American companies are spending millions of dollars to comply with the GDPR PricewaterhouseCoopers, 'GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey' (*PwC*, 23 January 2017) http://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html
[116] See, Bradford (n 14). pgs. 7-9.

i. Convergence requires rethinking where and how to apply economics

a. A common framework

It beyond of the scope of this paper to provide a detailed plan for an ideal antitrust policy for internet markets – this matter certainly deserves and is being subject to in-depth studies of its own.[117] Notwithstanding, the multiple variations of Google case-law shows how a hybrid US/EU competition policy may be a good framework to address the challenges of the internet economy. In particular, this policy would ideally incorporate the EU's more flexible approach to market definition and dominance with the US' more rigid approach to market exclusion and harm.

The lack of clear prices, the multi-sided nature of the businesses and the ever-shifting boundaries of markets will require American regulators to be more flexible in terms of the evidence required in the definition of relevant markets and on the assessment on whether companies possess market power.[118] The FTC seemed to be heading in that direction in its Google analysis, when it defined distinct relevant markets for general search and vertical search without the need for formal SSNIP/cross-elasticity, critical loss or other tests.[119] Equally, the definition of dominance and foreclosure may need to rely on more general evidence on switching costs, barriers to entry and others, as plaintiffs will hardly be able to present direct quantifiable evidence of price increases or output reduction in markets with zero pricing or multi-sided characteristics.[120] An analysis similar to the KinderStart case, affirming that no antitrust market exists when prices are zero, cannot

[117] See the recent OECD study on the matter - OECD (n 83).
[118] See also ibid., at 15.
[119] On the importance and techniques of relevant market definition in monopolization claims, see ABA Section of Antitrust Law (n 45). pgs. 599-602.
[120] ibid. pgs. 226-228. This is important because US Courts are reluctant to accept direct showings of exclusion as evidence of dominance. See ibid. at 227-228, quoting *McWane, Inc v FTC* (2015) 783 F.3d 814 (11th CIrcuit).

instruct an effective antitrust policy in an age where services are paid through a combination of data and attention.[121]

On the other hand, the EU's increasing focus on 'consumer choice' is over-inclusive. Creative destruction is the essence of competition and key to economic development.[122] This is particularly true in digital markets, where network effects are welfare enhancing and businesses are constantly improving their products with new features that exclude potential rivals in lateral products but that, normally, benefit consumers.[123] EU dominance investigations are too formalistic, especially on foreclosure assessment.[124] An optimal policy then will need to include at least part of the US approach to using economics as a tool to properly identify exclusion.[125]

---

[121] Although case law should (hopefully) evolve from the KinderStart framework as more cases reach courts, the decision is not alone in requiring plaintiffs to narrowly define relevant markets through cross-elasticity tests as a pre-condition to any antitrust lawsuit. See, for example, *Brown Shoe Co v United States* (1962) 370 SCt 294 (Supreme Court)., at 325 and *FTC v Lundbeck, Inc* (2011) 650 F.3d 1236 (8th Circuit). pgs. 4-6, citing many other cases.

[122] See Daron Acemoglu and James A Robinson, *Why Nations Fail: The Origins of Power, Prosperity, and Poverty* (1st edn, Crown Business 2013). p. 93-95. Jorge Padilla, 'The Role of Economics in EU Competition Law: From Monti's Reform to the State Aid Modernization Package' [2016] Concurrences Review. p. 10-11.

[123] See Todd (n 52). p. 85-91. It is interesting to notice that the EU itself recognizes this in merger review, however adopting a formal analysis to dominance investigations. An example is the Microsoft cases, in which the EU generally approved potential tying obligations in Microsoft/Skype and Microsoft/LinkedIn, however condemned them in the Windows Media Player investigation. This is inconsistent. See Ibáñez Colomo (n 41). Section 4.3.3.

[124] For example, on the Windows Media Player bundling case, the European Court of First Instance affirmed a formal theory of foreclosure based on the ubiquitous presence of WMP on Microsoft PCs. *Case T-201/04, Microsoft vs. Commission* (n 54). para.1058 See also Ibáñez Colomo (n 41). p. 11-12. The CJEU's *Case - C-413/14 P - Intel v Commission* [2017] CJEU ECLI:EU:C:2017:632. is a step in the right direction, though the Court may need to go further to revert the strong-presumption of illegality for certain other practices. It is telling that that the FTC has a team of more than 80 PhD economists, while the European Commission's team does not have even 30. See https://www.ftc.gov/about-ftc/bureaus-offices/bureau-economics/biographies and http://ec.europa.eu/dgs/competition/economist/contacts.html

[125] For example, analyses focused on whether companies had an actual incentive to exclude a given competitor from the market, combined with common-law doctrines, such as that of narrowing what qualifies as an antitrust injury, of remoteness (e.g. pass-on defenses) and a general concern in deterring welfare-enhancing conduct. See ABA Section of Antitrust Law (n

A good example of how this compromise between both jurisdictions can work in practice is the analysis of another Google litigation, now involving the UK mapping company Streetmap. In a summary, Streetmap accused Google of abusing its dominant position in general search to leverage its Google Maps business (and exclude Streetmap) by linking search queries with map search results. This blending of vertical and horizontal search results is similar to the other Google Shopping cases discussed above.

In a detailed opinion, which included expert testimony by economists and technology specialists, the British High Court dismissed the case. It affirmed that while Google's conduct could have contributed to the exclusion of Streetmap from the market, it did not entail an abuse of dominance and, if it did, it was objectively justified.[126] More specifically, the opinion initially accepted a presumption of Google's dominance in search[127] and affirmed that a condemnation depended on whether plaintiffs could prove anticompetitive foreclosure.[128] During trial, the Court found that: (i) Google systematically gave prominent placement to its own products at the expense of Streetmap;[129] and (ii) that Streetmap traffic declined significantly during the period.[130] However, the Court did not find a purposeful demotion of Streetmap by Google[131] (which would

45). at 729, quoting *RSA Media, Inc v AK Media Group, Inc* (2001) 260 F.3d 10 (1st Circuit); *Serpa Corp v McWane, Inc* (1999) 199 F.3d 6 (1st Circuit); *Greater Rockford Energy & Technology Corp v Shell Oil Co* (1993) 998 F.2d 391 (7th Circuit).

[126] *Streetmap EU Ltd v Google Inc & Others* (2016) 2016 253 (EWHC). Para. 177.

[127] The Court affirmed this presumption based on Google market share of 75%-85% and as a way to expedite the trial, holding that should it decide that Google's conduct was abusive, there could be a separate assessment on dominance. *ibid.* paras. 41-43. However, Google's high and stable market-share, combined with other qualitative factors such as brand recognition, economies of scale and scope, product portfolio, global presence and others justify a strong presumption of dominance against the company under the proposed framework.

[128] *ibid.* paras. 62-63.

[129] *ibid.* para. 102.

[130] *ibid.* paras. 130-133.

[131] *ibid.* para 79.

imply a clear intent to harm competition). As a result, rather than affirming a presumption of harm connected with Streetmap's exclusion from the market, the Court found that Streetmap's decline was mostly due to inferior quality.[132] It also affirmed that Google had an objective justification behind the integration of Google Search and Maps, and that Google could not structure its products in a less anticompetitive alternative.[133]

The Streetmap case is particular in many ways, not least because Google apparently had a much superior product and UK Courts are in between the US and the EU in terms of methodology. Nonetheless, it can demonstrate how the approach proposed herein does not imply that neither the EU nor the US must completely abandon the core principles that instructs their antitrust policies for some convergence to take place. Both jurisdictions can maintain, for example, different thresholds for the characterization of dominance, market foreclosure or consumer harm, limit or expand efficiency defenses for practices and maintain a more energetic enforcement in specific areas, such as those relating to the formation of the Single Common Market in the EU. This framework leaves enough flexibility for both sides to adapt their political priorities while speaking a common language in terms of methodology.[134]

[132] *ibid.* paras. 118-119. In particular, Streetmap did not: (i) recognize St as abbreviation of street (among other linguistic problems); (ii) have slippy maps (that move proportionally to zooming in or out); nor it (iii) recognize natural language searching (e.g. "where is the British Museum").
[133] *ibid.* paras 155-158.
[134] In the Streetmap case, EU Courts could, for example, affirm that if Google had a clear intent to harm competition, plaintiffs demonstrating preferential product placement and the decline of Streetmap would be enough to prove foreclosure. The US could maintain the more detailed examination of whether Google's actions drove Streetmap out of the market and whether there were countervailing efficiencies with the practice.

b. A window for convergence

Convergence, however, does not depend solely on the existence of a common framework but also on political motivation and opportunity. Politics is responsive to random events, so different triggers could be used to motivate a push for convergence.[135] Institutional changes, however, are more predictable and provide more concrete and coherent possibilities for integration. In this sense, a potential window may arise as the EU implements reforms aimed at increasing private antitrust litigation.

The differences in judicial behavior between the EU and the US are partly based on institutional design features of each jurisdiction and their focus on public or private litigation. The Chicago push was connected with the need to restrict private enforcement of competition laws in the US, where private parties lead antitrust litigation.[136] High litigation costs and treble damages may prohibitively raise the cost of doing business, in particular in the case of unilateral conduct where "grey cases" abound. Courts, therefore, resorted to economics and other reasoning[137] as

[135] For example, the recent Cambridge Analytica scandal in the US has renewed claims for a comprehensive privacy federal data protection regulation. Nonetheless, much of the push for new legislation is still focused on empowering user consent rather than imposing limitations as in Europe. Moreover, with Silicon Valley leading the US lobby industry it is likely that any new regulations may be watered down. See Steven Norton and Angus Loten, 'Facebook Hearings Illuminate Future of Business and Data Privacy' *WSJ* (San Francisco, 16 April 2018) 1; Olivia Solon and Sabrina Saddiqui, 'Forget Wall Street – Silicon Valley Is the New Political Power in Washington' *The Guardian* (San Francisco and Washington, 3 September 2017) 1.

[136] Between 2005 and 2015, private antitrust litigation outnumbered public litigation in the US by thousands of cases. See United States, 'Relationship between Public and Private Antitrust Enforcement - United States OECD Submission' https://www.ftc.gov/system/files/attachments/us-submissions-oecd-other-international-competition-fora/publicprivate_united_states.pdf and http://www.uscourts.gov/sites/default/files/statistics_import_dir/C02Jun14.pdf

[137] ABA Section of Antitrust Law (n 45) at 729, quoting *RSA Media, Inc. v. AK Media Group, Inc.* (n 125); *Serpa Corp. v. McWane, Inc.* (n 125); *Greater Rockford Energy & Technology Corp. v. Shell Oil Co.* (n 125).

gatekeepers to limit private litigation opportunities.[138] Opposingly, the EU relies on an administrative system of antitrust enforcement. This modifies Courts' incentives when setting judicial precedents, as they may rely on sophisticated gatekeepers to ensure that antitrust laws will not over-burden private parties by flooding them with dubious cases. It is rational for EU Courts to adopt more formal tests, deferring to specialized bureaucracies the complex economic assessments surrounding unilateral conduct.[139]

The EU system may change with the implementation of private damages Directive 2014/104/EU.[140] While these changes have important limitations,[141] increased private litigation should encourage Courts to develop better screening mechanisms to ensure that only actually harmed parties receive compensation. It is not surprising that the European Commission issued a guidance paper on how Courts should quantify harm in private antitrust lawsuits that makes use of diverse economic tools to calculate damages, pass-on defenses and others.[142] The use of the term

---

[138] *Brunswick Corp v Pueblo Bowl-O-Mat, Inc* (1977) 429 SCt 477 (Supreme Court). *Atlantic Richfield Co v USA Petroleum Co* (1990) 495 SCt 328 (Supreme Court)., see also William H Page, 'The Scope of Liability for Antitrust Violations' [1985] Stanford Law Review 1445. p. 1460.

[139] What EU Courts called "margin of assessment" or "margin of discretion". See Fernando Castillo de la Torre and Eric Gippini Fournier, *Evidence, Proof and Judicial Review in EU Competition Law* (Edward Elgar Publishing 2017)., at 76. Between 2004 and 2015 EU authorities started 2066 investigations, of which 907 ended in some form of enforcement (including agreements), a fraction of the US - European Commission, 'ECN - Statistics' http://ec.europa.eu/competition/ecn/statistics.html

[140] Directive 2014/104/EU on certain rules governing actions for damages under national law for infringements of the competition law provision of the Member States and of the European Union 2014 (OJ L 349, 5122014, p 1–19). For a summary of the changes see Sebastian Peyer, 'Compensation and the Damages Directive' (2016) 12 European Competition Journal 87., Section B.II.

[141] See, for example, Peyer (n 140)., Section D.

[142] See European Commission, 'Communication from the Commission on Quantifying Harm in Actions for Damages Based on Breaches of Article 101 or 102 of the Treaty on the Functioning of the European Union' http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:167:0019:0021:EN:PDF ; European Commission, 'Practical Guide on Quantifying Harm in Actions for Damages Based on Braches

'may' above is because EU Courts might adopt two different standards of analysis, one for public and another for private parties. For historical reasons, this did not take place in the US where the standards are the same for the FTC and for private litigators.[143] If this dual-standard takes place, the convergence window created by this institutional change will be limited.

It is not a coincidence that Streetmap exemplifies a potential convergence movement. While one may easily rely on the EU's more formal findings of dominance, the Court would step in fragile soil by simply presuming harm to Streetmap based on limited freedom of choice – the nature of the claim forced it to assess whether Streetmap's failure was connected with Google's actions. As more cases arise, judicial precedent will inevitably develop.[144]

ii. Data portability as a mitigating factor

While and if convergence does not take place, parties caught amidst this transatlantic rift may resort to some mitigating factors to help ease tensions and potential exposure. As concerns are mostly regarding American companies under threat of action by European regulators, this section defends data portability as a pragmatic and unilateral change these companies can adopt to

---

of Article 101 or 102 of the Treaty on the Functioning of the European Union - SWD(2013) 205' <http://ec.europa.eu/competition/antitrust/actionsdamages/quantification_guide_en.pdf>. The guidelines suggest, among others, comparison techniques such as (i) difference in differences (para 56) or prevented entry methods (para 200); (ii) linear interpolation or extrapolation (para. 67); (iii) regression analysis (para 92); and many variations of those techniques, such as: (iv) cost-based analysis and calculation of average profit margin per unit and of lost sales (para 191) or (v) finance-based analysis and evolution of profitability (para 115/197). See also RBB Economics and Cuatrecasas, Gonçalves Pereira, 'Study on the Passing-on of Overcharges' http://ec.europa.eu/competition/publications/reports/KD0216916ENN.pdf

[143] See generally, Justin Hurwitz, 'Chevron and the Limits of Administrative Antitrust' (2014) 76 U. Pitt. L. Rev. 209.

[144] This process may take less long than expected. Only in 2017 two British shopping comparison companies are privately suing Google for abuse of dominance, see James Titcomb, 'Price Comparison Site Kelkoo Takes Google to High Court over Abuse of Search Dominance' *The Telegraph* (London, 3 June 2017) 1; Martin Strydom, 'Foundem Leads Queue to Fight Google' *The Times* (London, 3 July 2017) 1.

address some of the concerns relating to data protection in the EU.[145]

Given the growing importance given to "freedom of choice" as a theory of harm, American companies would do well to pay specific attention to how the features of their products impact: (i) consumers' freedom to migrate to different, competing products; and (ii) interoperability between dominant platforms and products from competitors. Indeed, the EU has a long history of presenting antitrust charges against both American and non-American companies whenever specific features of product design hinder consumer freedom of choice and the development of market alternatives. This is one of the main theories of harm behind the Microsoft/Windows Media Player condemnation, where some of remedies required Microsoft to both develop a Windows version without a pre-installed Media Player and provide interoperability information to competitors. Similar concerns may be found in more recent cases. All the investigations opened against Google have a strong *limit the freedom of choice* component to it[146] and the Microsoft/LinkedIn merger only received EU approval after Microsoft agreed to behavioral commitments that prevent it from discriminating competitors and ultimately restrict freedom of choice.[147]

---

[145] A similar call for interoperability and adopting shared standards to ease exclusion concerns can be seen at OECD (n 83). p. 25.

[146] See European Commission, 'Antitrust: Commission Sends Statement of Objections to Google on Android Operating System and Applications' (20 April 2016) http://europa.eu/rapid/press-release_IP-16-1492_en.htm and European Commission, 'Antitrust: Commission Takes Further Steps in Investigations Alleging Google's Comparison Shopping and Advertising-Related Practices Breach EU Rules*' (14 July 2016) http://europa.eu/rapid/press-release_IP-16-2532_en.htm

[147] The merger was approved after Microsoft offered commitments that would: (i) ensure that pc manufacturers and distributors are free not to install LinkedIn on Windows; (ii) allow competing professional social networks to maintain current levels of interoperability with Windows; and (iii) grant competing professional social networks access to Microsoft gateway for developers. Again Commissioner Vestager emphasized how such commitments were important to ensure freedom of choice: "*Today's decision ensures that Europeans will continue to enjoy a freedom of choice between professional social networks*." European Commission, 'Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions' (6 December 2016) http://europa.eu/rapid/press-release_IP-16-4284_en.htm

Assuring interoperability translates well with European concerns that super-dominant companies are not unduly restricting market entry through illegal action. US tech Companies could, for example, have an institutionalized channel through which rivals may require access to certain features of the platform, raising awareness to potential restrictive practices they did not previously recognize. However, increased interoperability initiatives are insufficient to remedy pure excessive pricing prosecutions like the one Facebook is currently facing in Germany, and may even risk leading to data protection violations of its own. In such cases, an approach that could be explored by US tech companies is to emphasize the role of data portability mechanisms as a way to limit customer lock-in. Authorities in Europe are getting more and more concerned about the role of data: (i) as a barrier to entry; and (ii) in increasing switching costs. A well-established data portability system could be a defense argument to both claims. Major platforms such as Google and Facebook already have systems which allow for the extraction of data, the same being said about specific data scraping software which are made available for companies. However, these systems currently only allow for the download of limited data, are not widespread and users remain largely misinformed about the existence of these functionalities.[148]

Article 20 of the GDPR tries to change this dynamic by creating a right to data portability that the EC believes '*will support the free flow of personal data in the EU and foster competition between controllers'.*[149] Instead of fighting these provisions, companies could embrace this as a

[148] See, Rob Pegoraro, 'Web Companies Should Make It Easier to Make Your Data Portable: FTC's McSweeny' *USA Today* (Lisbon, 12 November 2017) https://www.usatoday.com/story/tech/columnist/2017/11/12/web-companies-should-make-easier-make-your-data-portable-ftcs-mcsweeny/856814001/ and Christopher Mims, 'Facebook Data Harvest Yields Confusing Maze' *Wall Street Journal* (14 April 2018) 1.

[149] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf at 3.

unique opportunity to collaborate with their European counterparts. They could, for example, develop a joint-standard to be used across the industry, which would facilitate both downloading personal data and also transferring it to third-parties (when required by the user).[150] This would demonstrate a commitment to upholding European values and weaken *exploitative abuses* claims by authorities. In exchange, European authorities could at least consider this an important mitigating factor in an eventual prosecution.

IV. CONCLUSION

Market protectionism is widespread and on the rise since the 2008 financial crisis. This paper cannot completely rule out protectionism as a force behind Europe's approach to data protection and antitrust enforcement.[151] However, this article adds a different perspective by arguing that those initiatives reflect, at least in a relevant part, historical differences in the shaping of data protection and competition policies in the EU and the US. As Europeans explore more in depth the interconnection between both policies (currently still at its early stages), the differences between both jurisdictions should only widen.

Nonetheless, if the current USD 250 billion worth of digital trade[152] and the rapid (if problematic) negotiations of a new EU/US Safe Harbor for data transfers imply something is that companies cherish some convergence or at least proper rationalization in this arena. While it may

---

[150] As the EC itself suggested, see ibid. at 14.

[151] There is evidence suggesting that protectionism is not taking place in EU merger review, even in relation to high-technology sectors. See Bradford, Jackson and Zytnick (n 2). at 187. However, the protection of EU companies' competitiveness has always been at the forefront of European market regulation. Bradford (n 14). at 40-42.

[152] Roslyn Layton, 'Europe's Protectionist Privacy Advocates' *Wall Street Journal* (9 March 2016) http://www.wsj.com/articles/europes-protectionist-privacy-advocates-1457566423

be optimal for different societies to have at least partially different rules (including in relation to competition and data protection policies in digital markets), this divergence can become burdensome and lead to unexpected trade conflicts.

American authorities and companies need to consider historical differences if they intend to influence policy-making in Europe (and vice-versa). If not out of respect for European traditions, at least due to a pragmatic view on international relations. Otherwise, EU authorities can easily resort to these cultural distinctions as an underpinning to disqualify American opinions as disconnected from European realities and values – failing to incorporate legitimate concerns in local policy making. The same holds true for Europeans, who must do more to dispel concerns of political targeting. A failure by both sides to understand their significant policy differences may hurt businesses and consumers alike.

All the suggestions proposed herein are just one more input to the complex topic of how to shape antitrust and data protection policies to address the concerns of the digital age, a field that will still be receiving contributions for many years to come.

Essay 2:
Towards a Layered Approach to Relevant Markets in Multi-Sided Transaction Platforms*

INTRODUCTION

The rise of the digital economy spurred interest in the application of antitrust to so-called two-sided or multi-sided platforms—an area that has attracted the attention of academics and policymakers[1] Multi-sided platforms challenge the traditional tools used in antitrust analysis, requiring the rethinking of long-established doctrines and leading to much controversy on whether there is need for the re-design of antitrust policy around the world.[2] Much of the focus is on understanding how economic incentives change in markets with pervasive direct and indirect

---

* This article was originally published in the Antitrust Law Journal, Volume 83, Issue 2, Pages 429-481 (2020). It is reprinted in this Dissertation in accordance with the American Bar Association Copyright Policy. In addition, this author was co-authored with Professor Caio Mario da Silva Pereira Neto, whom I thank deeply for the partnership.

[1] For a seminal paper, see William F. Baxter, *Bank Interchange of Transactional Paper: Legal and Economic Perspectives*, 26 J.L. & ECON. 541 (1983) and, equally important, Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report*, 37 RAND J. ECON. 645 (2006). For a literature review, see David S. Evans & Richard Schmalensee, *The Antitrust Analysis of Multisided Platform Businesses*, *in* 1 THE OXFORD HANDBOOK OF INTERNATIONAL ANTITRUST ECONOMICS 404 (Roger D. Blair & D. Daniel Sokol eds., 2014). For a more recent take, see OECD, RETHINKING ANTITRUST TOOLS FOR MULTI-SIDED PLATFORMS (2018), www.oecd.org/daf/competition/Rethinking-antitrust-tools-for-multi-sided-platforms-2018.pdf; Michael Katz & Jonathan Sallet, *Multisided Platforms and Antitrust Enforcement*, 127 YALE L.J. 2142 (2018).

[2] *See* OECD, *supra* note 1; Jonathan B. Baker, Jonathan Sallet & Fiona Scott Morton, *Unlocking Antitrust Enforcement*, 127 YALE L.J. 1916 (2018) (a *Yale Law Journal* special edition on antitrust enforcement).

network externalities and more complex pricing structures than traditional vertical supplier-consumer industries (including zero pricing markets).[3]

This once theoretical debate quickly moved to real life. Germany amended its antitrust laws to better address multi-sided markets.[4] Google now holds record fines for antitrust violations after three consecutive convictions in the European Union[5]—decisions in which much of the criticism focused on relevant-market definition and proof of harm. In the United States, the Supreme Court finally stepped into the debate with its decision in *Ohio v. American Express* (*Amex*).[6] As presented in Part I, the heart of that controversial five-to-four split vote[7] was the question of how to delineate relevant markets in cases involving transaction platforms: while the majority affirmed that any two-sided transaction platforms should always be considered a single

[3] *See, e.g.*, David S. Evans, *The Antitrust Economics of Free*, COMPETITION POL'Y INT'L, Spring 2011, at 71; Michal S. Gal & Daniel L. Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement*, 80 ANTITRUST L.J. 521 (2016).

[4] Falk Schoening et al., *Digital Is Trump!—Market Definition and New Dominance Criteria for Digital Markets*, HOGAN LOVELLS: FOCUS ON REGULATION (June 22, 2017).www.hlregulation.com/2017/06/22/digital-is-trump-market-definition-and-new-dominance-criteria-for-digital-markets/.

[5] Press Release, Eur. Comm'n, Antitrust: Commission Fines Google €1.49 Billion for Abusive Practices in Online Advertising (Mar. 20, 2019) (IP/19/1770) (linking to all three Google fines). For a discussion of the second fine, see Randal Picker, Google Android *Antitrust: Dominance Pivots and a Business Model Clash in Brussels*, CPI ANTITRUST CHRON., Dec. 2018, at 1.

[6] Ohio v. Am. Express Co., 138 S. Ct. 2274 (2018) (*Amex*).

[7] Indeed, the case not only split the U.S. Supreme Court but much of American antitrust academia, as shown by the number of amicus briefs filed by professors such as Herbert Hovenkamp, Harry First, Einer Elhauge, Eleanor Fox et al.; David Evans and Richard Schmalensee, and Richard Epstein and Joshua Wright offered divergent views on how the Court should decide the case. *See* Brief of 28 Professors of Antitrust Law as *Amici Curiae* Supporting Petitioners, Ohio v. American Express Co., No. 16-1454 (Dec. 14, 2017) (including Professors Hovenkamp, First, Elhauge, and Fox, among others); Brief for *Amici Curiae* Prof. David S. Evans and Prof. Richard Schmalensee in Support of Respondents, Ohio v. American Express Co., No. 16-1454 (Jan. 23, 2018); Brief for *Amici Curiae* Antitrust Law & Economics Scholars in Support of Respondents, Ohio v. American Express Co., No. 16-1454 (Jan. 23, 2018) (including Professors James C. Cooper, Richard Epstein, Tad Lipsky, David Teece, and Joshua Wright).

relevant market, the minority focused solely on payment services provided to one side of the market (i.e., merchants). Given the importance of relevant market definition as an analytical tool in antitrust analysis, it is no surprise that these opposite views led to different conclusions on whether American Express (or, in the future, Google, Amazon, Apple, or any other company operating transaction platforms) had market power and whether parties proved an antitrust infringement punishable by law.

Following an overview of the literature on multi-sided platforms (Part II), this article challenges both the majority and the minority opinions in *Amex*. It proposes a novel, multi-layered approach to relevant market definition that is better aligned with the established view that antitrust analysis should focus on the competitive constraints faced by firms (Part III). In particular, using the electronic payments market as reference, it demonstrates how multiple relevant markets may co-exist within a single transaction platform—depending on the focus of the analysis and the strength of network effects. In doing so, it challenges the *Amex* majority's opinion (which reflects part of the literature) that transaction platforms *always* lead to the definition of a single relevant market encompassing both sides of the platform. On the contrary, in some transaction platforms, where firms are not particularly constrained by indirect network externalities, some players indeed operate as if in one-sided markets. This, however, does not mean that the minority opinion is correct. The dissent led by Justice Breyer ignores that some players (normally the platforms owners) are focused on balancing the overall platform and should not be required to consider in isolation the impacts of their conduct on a single side of the network. Our view may be considered a bridge between the two most important strains in the literature on the topic, the one defending

the prevalence of one multi-sided market[8] and the other that favors multiple, one-sided markets.[9] This view is particularly important to instruct antitrust scholars and lower courts on when cases warrant a multi-sided analysis—meaning that *Amex* is the applicable precedent—and when they should look for alternative frameworks.

In other words, this article proposes a pragmatic approach to relevant market definition that is based on two opposite findings. On one hand, as well recognized, economic constraints on transaction platforms come not only from substitutability of products/services traditionally considered in relevant market definition, but also from direct and indirect network effects that may limit competitive strategies adopted in either side of the platform—a process that pushes towards defining a single multi-sided relevant market. On the other hand, as less acknowledged, these very same platforms may be structured in ways that limit a firm's (or a set of firms') exposure to these network effects, so that they are insufficient to limit the firm's ability to raise prices on a single-side of the platform without passing the price derived from users on one side of the platform to users on the other side of the platform—justifying an analysis focused solely on this impacted side.

By focusing the analysis on a firm's ability to profitably raise prices on one side of the platform without being materially constrained by the other side, this article argues that a single transaction platform may be better interpreted as encompassing different layers of competition, justifying the definition of a single two-sided relevant market (e.g., the platform), as well as multiple one-sided relevant markets (e.g., acquirers, issuers). Moreover, these different layers interact in a dynamic way. This somewhat simple point has surprisingly been overlooked by the

[8] *See, e.g.*, David S. Evans & Michael Noel, *Defining Antitrust Markets when Firms Operate Two-Sided Platforms*, 2005 COLUM. BUS. L. REV. 667; Lapo Filistrucchi et al., *Market Definition in Two-Sided Markets: Theory and Practice*, 10 J. COMPETITION L. & ECON. 293 (2014).
[9] *See, e.g.*, Dennis W. Carlton & Ralph A. Winter, *Vertical Most-Favored-Nation Restraints and Credit Card No-Surcharge Rules*, 61 J.L. & ECON. 215 (2018); Katz & Sallet, *supra* note 1.

more recent scholarship addressing the question. In doing so, this article creates a bridge between the majority and the minority opinion in *Amex*. It acknowledges that two-sided transaction platforms are particularly prone to indirect network externalities and, as such, generally tend to constitute a single two-sided market, at least at the level of inter-platform competition. However, this insight is not definitive and, most importantly, it does not explain the full competitive dynamics in play. An in-depth analysis of the particular economic constraints faced by players in a given industry may provide good reasons to look further and define single-sided relevant markets even within transaction platforms. This balancing depends essentially on the structure of the platform, the existence of intra and inter-platform competition, and the intensity of network effects in the different layers of this complex competitive environment.[10]

Building on this perspective, the article then moves on to analyze the rich experience of the European Union and Brazil in the application of competition law to electronic payments (Part IV). While diverging from the United States on relevant market definition, both the European Union's and Brazil's antitrust case law involving the payments networks of Visa, Mastercard, and even American Express, seem to better account for the complex competitive dynamics in these markets. Indeed, it seems puzzling that the debate in the United States has not taken into account the rich international experience regarding the electronic payment's industry.

After analyzing the international experience on the electronic payments industry, the article moves on to translate our general approach into a specific methodology to define relevant markets in two-sided transaction platforms, proposing a four-step structured framework on how authorities

[10] In doing so it reflects long-established traditions that the antitrust analysis of complex multi-sided markets requires a consideration of how intra-platform rules impact actual market conditions, given that some restrictions may help promote transparency and increase competition. See, for example, Justice Brandeis's opinion in *Chicago Board of Trade v. United States*, 246 U.S. 231, 232 (1918).

should evaluate the competitive dynamics in these industries (Part V). This framework is both more comprehensive than most alternative propositions on the topic and provides clearer guidelines that can be followed by policymakers and scholars facing the challenge of defining relevant markets when complex platforms are involved. Part VI outlines how this multi-layered approach may work in cases involving other transaction platforms, such as marketplaces and ride-sharing apps.

I. THE SUPREME COURT DECISION IN AMEX

i. Electronic Payments Markets and the Charges Against *Amex*

American Express is a vertically integrated payment card system. As the platform owner, it issues its own cards and it has direct relationships with the merchants for acquiring payments.[11] Visa and Mastercard, on the other hand, only coordinate the payments system. On one side of the platform, they rely on banks to issue cards, which also remain responsible for setting membership fees, interest rates, and the terms of loyalty programs. On the other side, they rely on third-party acquirers (which may or may not be banks, depending on the country) to develop relationships with merchants and capture transactions.

The different business models create different economic incentives. Although the Supreme Court and the Second Circuit decisions acknowledged this difference, they failed to properly understand how this difference shapes the incentives of different players and how these incentives should also shape discussions on the definition of relevant markets definition or the impact on

[11] United States v. Am. Express Co., 838 F.3d 179, 188–89 (2d Cir. 2016), *aff'd sub nom*. Ohio v. Am. Express Co., 138 S. Ct. 2274 (2018) (*Amex*); DAVID S. EVANS & RICHARD SCHMALENSEE, PAYING WITH PLASTIC: THE DIGITAL REVOLUTION IN BUYING AND BORROWING 1–8 (2d ed. 2005).

consumer welfare. The failure of the courts to understand the theoretical implications of their rulings is worrisome because it creates legal uncertainty and deprives lower courts of proper guidance with regards to when the precedent is applicable. Indeed, the Supreme Court itself failed to even mention *Amex* in *Apple Inc. v. Pepper*,[12] a two-sided markets case it decided the following term.

Credit card markets are complex, but the theory of harm behind the charges against American Express was simple.[13] The company used contractual clauses to prevent merchants from "steering" clients away from American Express' products. As the second circuit explained, American Express barred merchants from: "(1) offering customers any discounts or nonmonetary incentives to use credit cards less costly for merchants to accept, (2) expressing preferences for any card, or (3) disclosing information about the costs of different cards to merchants who accept them."[14] These practices could harm consumers if they inhibited entry or suppressed competition from rival networks and, thus, lead to higher prices or lower output.[15]

[12] Apple Inc. v. Pepper, 139 S. Ct. 1514 (2019).
[13] *See* Randy Picker, *With Amex Ruling, Modern IO Theory Makes Important Inroads with SCOTUS*, PROMARKET (June 28, 2018), promarket.org/amex-ruling-modern-io-theory-makes-important-inroads-scotus/.
[14] *American Express Co.*, 838 F.3d at 184.
[15] This is a practice that exists in Europe, for example, where merchants sometimes accept credit cards but charge a fee, increasing the final cost to the consumer vis-à-vis payments with other credit cards, debit cards, or cash. The same thing happens to American Express, as some retailers charge users more when they use American Express than when they use Visa or Mastercard. *See* Rupert Jones, *Credit Cards: Is This the End of the Great Rip-Off?*, THE GUARDIAN (Jan. 13, 2018), www.theguardian.com/money/2018/jan/13/credit-card-surcharge-debit-ban (describing how the practice has been banned in the United Kingdom but not in the rest of Europe).

ii. The Majority's Decision's Limited Focus on a Single Two-Sided Relevant Market

Justice Thomas's majority's opinion in *Amex* quickly became a landmark for antitrust cases involving multi-sided platforms.[16] Relevant markets are the lenses through which competition authorities and courts can assess the existence of market powers and the effects of specific conducts.[17] In many cases, market definition is key to the finding of infringement—different lenses highlight different aspects of the conduct and lead to different conclusions. This is what took place in *Amex*. While the majority argued for the definition of a single relevant market for the "two-sided transaction platform" of credit cards; the minority argued that the relevant market should be narrowly defined to consider only the services rendered to merchants, focusing on one side of the platform.

Drawing on the literature on multi-sided platforms,[18] the majority opinion distinguished between "two-sided transaction platforms" and "two-sided non-transaction platforms." The distinctive character of a "two-sided transaction platform" would be the fact that the platform is used to match sides (e.g., cardholder and the merchant in the case of payment cards) and generate a single transaction. In this sense "transaction platforms (…). cannot make a sale to one side of the platform without simultaneously making a sale to the other."[19] In contrast, "two-sided non-

[16] *See* Ted Tatos, *Relevant Market Definition and Multi-Sided Platforms After* Ohio v. American Express*: Evidence from Recent NCAA Antitrust Litigation*, 10 HARV. J. SPORTS & ENT. L. 147 (2019) (discussing how *Amex* shaped claims of multi-sided market definition in an NCAA case).
[17] *See* 1 ABA SECTION OF ANTITRUST LAW, ANTITRUST LAW DEVELOPMENTS 224–25 (8th ed. 2017) (quoting, among others, Spectrum Sports, Inc. v. McQuillan, 506 U.S. 447 (1993); United States v. Grinnell Corp., 384 U.S. 563 (1966)).
[18] *E.g.*, Evans & Noel, *supra* note 8; Filistrucchi et al., *supra* note 8; Benjamin Klein et al., *Competition in Two-Sided Markets: The Antitrust Economics of Payment Card Interchange Fees*, 73 ANTITRUST L.J. 571 (2006).
[19] Ohio v. Am. Express Co., 138 S. Ct. 2274, 2277 (2018).

transaction platforms" would match different customer groups but would not generate a single transaction (e.g., newspapers selling advertising and subscriptions).

According to the Court, "transaction platforms" are particularly prone to intense network effects ("pronounced indirect network effects and interconnected pricing and demand"[20]), as the value of the platform to one side increases with the expansion of the other side. Indeed, cardholders perceive value in acquiring a payment card from a brand that is accepted by most merchants, and merchants perceive value in accepting brands used by most cardholders. As a result, platform owners are always concerned with the balance between the two sides and cannot increase prices to one side (say merchants) without risking losing customers on the other side (cardholders). Still according to the majority, these mutual constraints are so strong that "credit-card networks are best understood as supplying only one product—the transaction—that is jointly consumed by a cardholder and a merchant."[21] Therefore, the court concluded that two-sided markets for credit-card transactions should be analyzed as whole.

This definition of a single relevant market was crucial to the majority's conclusion that American Express had not violated Section One of the Sherman Act. Indeed, as the Court viewed the case, the impact of anti-steering provisions on the merchant side was necessarily limited: American Express (or any other rational player) will always be concerned with the value of the entire platform and will account for the two sides of the market. As a result, the anti-steering provisions should be seen as only one piece of a broader strategy to generate value as the company attracts wealthier customers through higher cardholder rewards, which are offset by higher merchant fees.

[20] *Id.* at 2286.
[21] *Id.* at 2278.

The majority's argument acknowledges that multi-sided platforms with intense network effects may need to be analyzed as a single market. Understanding the inter-relation of the different sides of a given platform and the competitive dynamics between different platforms is certainly a relevant part of applying competition law to multi-sided markets. However, the majority oversteps, uses a broader language than necessary, and apparently argues for the application of this "single market" approach to all "two-sided transaction platforms." In doing so, it fails to recognize that even "transaction platforms" are made up of players with different incentives and may encompass different competitive dimensions that must be considered.

As discussed below, credit-card networks seem especially complex and would deserve a more thorough analysis than Justice Thomas's 20-pages afforded. One dimension of competition between these networks is indeed at the inter-platform level. However, other competitive dimensions, largely ignored by the majority, are also important.

iii. The Minority's Limited Focus to One Side of the Market

The minority's view in *Amex* also has significant shortcomings. The dissenting opinion led by Justice Breyer argues for a narrow one-sided relevant market, as if network effects played no material role in this discussion. The opinion makes a valid point when it separates credit card markets according to "merchant-related card service[s]" and "shopper-related cards service[s]"[22], identifying other potential dimensions of competition within the platform. However, the opinion fails to recognize the differences between the business model of American Express and Visa/Mastercard and, more importantly, how network effects generate potentially different economic incentives to players within the networks.

[22] *Id.* at 2291.

In addition, the minority also errs when it simplifies credit card markets and analogizes them to newspapers[23] or other markets with complementary goods such as gasoline and tires.[24] Justice Breyer affirms that "[l]ike gasoline and tires, both [merchant-related and shopper-related card services] must be purchased for either to have value."[25] Complementary goods, however, are different from a match-making platform. As explored in more detail below, the "pronounced indirect network effects and interconnected pricing and demand"[26] of a vertically integrated payment system like American Express cannot be simply dismissed. These effects strengthen the case for considering the whole platform competition as a single relevant market.

In the effort to justify their respective conclusions, both the majority opinion and the dissent fail to acknowledge how a complex market like electronic payments may be composed of different layers of competition. Multi-sided platforms may encompass multiple competitive dynamics occurring simultaneously—different players have different economic incentives. This requires a more subtle, layered approach to market definition and the use of multiple lenses to understand the competitive effects of certain conducts. This is not solely a theoretical exercise. Companies and courts have struggled to identify the presence of single-sided or multi-sided markets and to comprehend how different economic incentives impact competitive dynamics ever since Justice Brandeis affirmed that the rule of reason applied to these types of markets in *United States v. Chicago Board of Trade*.[27] *Amex* is one of the latest and potentially the most important iteration of this debate to date. Nonetheless, the lack of a cohesive rationale prevents companies and courts

[23] *Id.* at 2295 (quoting Times-Picayune Publ'g Co. v. United States, 345 U.S. 594, 610 (1953)).
[24] *Id.* (for primary and secondary markets, citing Eastman Kodak Co. v. Image Tech. Servs., Inc., 504 U.S. 451, 463 (1992)).
[25] *Id.* at 2296.
[26] *Id.* at 2286.
[27] Bd. of Trade of Chi. v. United States, 246 U.S. 231, 232 (1918).

from better differentiating cases where *Amex* is an applicable precedent from those where a different framework is warranted.

II. RELEVANT MARKETS IN TWO-SIDED PLATFORMS: STATE OF PLAY

The rise of digital platforms brought about a significant increase in the scholarship on the industrial organization of two-sided markets and its impact on antitrust policy.[28] Multi-sided platforms solve a transaction-cost problem that stops agents belonging to different groups from getting together. In doing so, they act as a catalyst, creating value for all groups.[29] As this scholarship explains, multi-sided markets present three key features: (1) strong indirect network effects between the different groups (the externalities that lead to feedback effects can run one or both ways);[30] (2) their price structure, and not only price level, impacts the total volume of demand to a given platform;[31] and (3) platforms (not the groups of users they connect) normally internalize the network externalities (and diminished transaction costs) they generate.[32] For these features to

[28] For a seminal analysis on the formation and the incentives around multi-sided payment platforms, see Baxter, *supra* note 1. For more modern, reference models on strategic behavior in multi-sided markets, see Mark Armstrong, *Competition in Two-Sided Markets*, 37 RAND J. ECON. 668 (2006); Bernard Caillaud & Bruno Jullien, *Chicken & Egg: Competition Among Intermediation Service Providers*, 34 RAND J. ECON. 309 (2003); Evans & Noel, *supra* note 8; David S. Evans, *Some Empirical Aspects of Multi-Sided Platform Industries*, 2 REV. NETWORK ECON. 191 (2003); Alan S. Frankel, *Monopoly and Competition in the Supply and Exchange of Money*, 66 ANTITRUST L.J. 313 (1998); Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. EUR. ECON. ASS'N 990 (2003).

[29] *See* Evans & Schmalensee, *supra* note 1, at 405; Baxter, *supra* note 1, at 576.

[30] Filistrucchi et al., *supra* note 8, at 296.

[31] Rochet & Tirole, *supra* note 1, at 647, 650. Price levels are roughly the total price charged by the platform to the two-sides (the overall cost of the service is x). The structure is roughly the decomposition/ratio of the price level between the buyer or seller (side a pays z, side b pays y, z+y=x). Characterized as roughly because these values need to be expressed in the same unit of measurement. Filistrucchi et al., *supra* note 8, at 299.

[32] Rochet & Tirole, *supra* note 28, at 994; Rochet & Tirole, *supra* note 1, at 646. Platform externalities can be divided between usage and membership. Usage externalities are positive indirect network externalities that benefit both sides of the platform whenever the system is

apply, platforms must have some market-power in relation to both sides and should be able block side-payments between the parties. Otherwise, the side being charged the most could simply pass-through the extra cost and defeat the incentives set by the price structure.[33]

In order to maximize profits, platforms define a price structure that partly reflects the ratio of elasticities between the different interconnected sides.[34] The platform normally charges more on the inelastic side of demand (usually the side not making the usage decision).[35] More interestingly, the ratio of elasticities of demand may be such that it is profitable for the platform to charge a below marginal cost to one side, locking in that demand so as to "recoup" by charging higher prices to the inelastic side.[36] Equally, platforms may find it profitable to induce (or block) steering, that is, by adjusting the price structure the platform may lock-in buyers or sellers in a way

---

used—the platform diminishes their immediate transaction costs. Usage externalities may be negative to one side—think of advertisers and internet users. Membership externalities are also generally positive indirect network externalities that benefit both sides of the platform: more members of the other category join the network, the higher the number of potential transactions the platform can generate. These also impact price structures, as platforms can charge membership fees (e.g., annual fees to have credit cards) and usage fees (e.g., interchange fees or merchant discount rate or others). Membership externalities, however, can become negative when congestion or other problems increase intra-platform search costs or other costs that diminish the chance of an agent finding its best counterpart—so platforms try to balance between positive and negative externalities. There is usually a trade-off between membership and usage fees. Finally, membership and usage decisions are usually taken at different times, and sometimes usage decisions are taken by only one side. Caillaud & Jullien, *supra* note 28, at 315; Özlem Bedre-Defolie & Emilio Calvano, *Pricing Payment Cards*, AM. ECON. J.: MICROECONOMICS, Aug. 2013, at 206, 208; David S. Evans, *Basic Principles for the Design of Antitrust Analysis for Multisided Platforms*, 7 J. ANTITRUST ENFORCEMENT 319, 322 (2019).

[33] Filistrucchi et al., *supra* note 8, at 299 ; Rochet & Tirole, *supra* note 28, at 1018–20.

[34] This ratio reflects the price elasticities of each side plus the marginal network effects of that side in attracting opposite demand. Klein et al., *supra* note 18, at 579, 582.

[35] Bedre-Defolie & Calvano, *supra* note 32, at 218; Rochet & Tirole, *supra* note 28, at 997–98.

[36] Evans & Schmalensee, *supra* note 1, at 412; Caillaud & Jullien, *supra* note 28, at 314–15; Rochet & Tirole, *supra* note 1, at 658–59. It is important to note that this recoupment is not a cross-subsidy. If the price structure is optimal, a firm will not be able to enter the market by simply "cream skimming" the profitable side as it will not be able to generate the indirect network effects that enabled the price structured in the first place. Julian Wright, *One-Sided Logic in Two-Sided Markets*, 3 REV. NETWORK ECON. 44, 50–51 (2004).

that hinders or even blocks multi-homing in either or both sides of the market (due to the indirect externalities).[37] That can be seen as a form of inter-platform competition, but may also be an effective exclusionary conduct by locking demand in a dominant platform, depending on the circumstances.[38]

Understanding these characteristics is key, in particular the distinction between price structure, price levels, and how they impact indirect network effects. For example, such distinction allows us to separate multi-sided platforms from traditional complementary goods (the gasoline and tire manufacture example given by Justice Breyer in *Amex*). First, producers of complementary goods do not necessarily have control over the price level or the price structure of the different goods. Gasoline and tire producers are normally independent economic agents and, as such, normally take the price of the complement as a given.[39] Second, in the case of complementary goods, the same group of consumers acquires both products and will take into account the total price level, while in multi-sided platforms, different groups of users will pay different prices to use the platform.[40] Third, and most importantly, the increase in demand for one product does not increase the overall utility of the other product—i.e., there is no indirect network effect between complementary products. Indeed, it is hard to argue that selling more gasoline makes tires generally more useful to car owners. All cars still use the same four tires, and the

[37] Armstrong, *supra* note 28, at 678–80; Rochet & Tirole, *supra* note 28, at 1000–02. Platforms have individual incentives to do so even if strong anti-steering practices risk diminishing overall welfare by raising retail prices above the competitive levels to all. Bedre-Defolie & Calvano, *supra* note 32, at 218; Carlton & Winter, *supra* note 9, at 215–17, 227–29.
[38] OECD, *supra* note 1, at 120.
[39] Rochet and Tirole also discuss this possibility, arguing that in many cases firms are price-takers on one side, not having the power to alter the price structure of the market. Rochet & Tirole, *supra* note 1, at 648–49. For an in-depth, historical analysis on complement goods and bundling practices, see Randal C. Picker, *The Razors-and-Blades Myth(s)*, 78 U. CHI. L REV. 225 (2011).
[40] Filistrucchi et al., *supra* note 8, at 296–97.

owner will need to change tires every so often, so that consumers will not perceive increased utility in the use of tires and will not be willing to pay more for them. In other words, even if a conglomerate producing both goods decides to increase the price of gasoline to subsidize the price of tires, the impact on demand will come mostly from the impact on the price level (i.e., the overall change in cost of the gasoline/tire bundle),[41] not because the change in the ratio between prices impacts the amount of gasoline on the market and, this alone, increases the demand for tires. Complements have no bandwagon effect.[42]

This, however, is what happens in a market like credit cards. The fact that American Express gives consumers (more) rewards whenever they acquire something encourages consumers to shift towards American Express vis-à-vis other payment methods. The increase in the number of American Express users encourages more merchants to join the network, and vice-versa. This aspect of a platform distinguishes them from Justice Breyer's gasoline and tires example. Merchants extract more utility from a payment network as the number of cardholders grows (i.e., number of potential transactions in that network will grow). This additional value perceived by merchants is not internalized by cardholders, just as additional value perceived by cardholders is not captured by merchants (i.e., as each group maximizes its own interests, they are indifferent to the increased value generated to the other group). This is the reason why such effects are considered externalities.[43] Nevertheless, as the number of potential transactions grows and both

[41] Even if accounting for the fact that over the long-term different users consume cars and tires in different proportions. This system, for example, would subsidize infrequent drivers at the expense of those who drive more and must consume more gasoline.
[42] *See* Robert S. Pyndick, Mass. Inst. of Tech., Sloan Sch. of Mgmt., Industrial Economics for Strategic Decisions Lecture Notes on Pricing 12–15 (Aug. 2015), web.mit.edu/rpindyck/www/Courses/Pricing_15.pdf (providing a summary explanation).
[43] Lapo Filistrucchi, *Two-Sided vs. Complementary Products*, CPI ANTITRUST CHRON., Sept. 2018, at 3.

sides are willing to pay more to join and use the network (i.e., the utility derived from the network is higher), the value of American Express as a platform equally grows and it can extract more of the surplus generated by these transactions.[44] The fact that American Express internalizes a significant part of this added value is also a key distinction of platforms vis-à-vis complementary goods.[45]

These and other derived insights led to a number of challenges to traditional antitrust policy tools, in particular in relation to market definition, assessment of market power, exclusion and potential efficiencies.[46] Competition enforcers and courts define relevant markets for an instrumental reason, not as an end to itself. Markets are defined to assess competitive constraints ("commercial realities") that prevent or enable firms to raise prices, diminish output, or lower quality.[47] The main focus of SSNIP or other similar tests is to assess demand or supply side substitutability.[48] These, however, do not traditionally work in the same way in the case of multi-sided markets because of the interconnected nature of demand.[49] Indirect network effects act as an effective competitive constraint on the firm running the platform (as if increasing the price elasticity of both sides) and an unbalanced platform is less valuable.[50] This complicates the

[44] Bedre-Defolie & Calvano, *supra* note 32, at 218; Klein et al., *supra* note 18, at 594.
[45] *See* Rochet & Tirole, *supra* note 28, at 991; Joshua D. Wright & John M. Yun, *Burdens and Balancing in Multisided Markets: The First Principles Approach of* Ohio v. American Express, 54 REV. INDUS. ORG. 717, 732 (2019).
[46] For a general review, see Evans & Schmalensee, *supra* note 1, at 420–26 (conduct in multi-sided market).
[47] Evans & Schmalensee, *supra* note 1, at 424; Filistrucchi et al., *supra* note 8, at 294–95.
[48] *See* Renata B. Hesse & Joshua H. Soven, *Defining Relevant Product Markets in Electronic Payment Network Antitrust Cases*, 73 ANTITRUST L.J. 709, 715–16 (2006).
[49] David S. Evans & Michael D. Noel, *The Analysis of Mergers that Involve Multisided Platform Businesses*, 4 J. COMPETITION L. & ECON. 663, 667 (2008).
[50] Evans & Noel, *supra* note 8, at 680–83.

definition of optimal prices when compared to traditional, one-sided business models[51] and justifies the rethinking of tools usually employed in relevant market definition.

The nature and strength of the indirect network effects should mark the distinction between a one-sided and a multi-sided market.[52] When the effects run only one way, markets may be deemed single-sided for the purposes of antitrust analysis, at least in relation to the side not impacted by network effects (in this case, traditional market definition tools normally apply). However, even in these cases, only the side of the platform that does not exert any pressure on the other is truly single-sided (e.g., in the case of newspapers, advertisers may not affect readership, so it may be appropriate to analyze advertising separately); the side exerting some pressure on the other must be analyzed as an interrelated market (e.g., changes in readership of newspapers affects pricing to advertisers, constraining pricing decisions at the readers' side and requiring an integrated analysis).[53] When the indirect network effects are strong and run both ways, then platforms are indeed balancing both sides of the market in a given interaction. In this case, market definition should account for both sides of the platform at once. The problem has been in trying to translate these teachings into practice and avoiding overbroad or excessively narrow definitions that lead to false negatives or false positives in antitrust enforcement.

---

[51] For example, in the case of multi-sided platforms charging only usage fees, while the optimum price for a one-sided monopolist follows a traditional Lerner formula (price is inversely related to demand elasticity), the multi-sided optimal pricing structure is the ratio of elasticities between both sides. This is because the platform has to balance the demand from both sides. *See* Rochet & Tirole, *supra* note 28, at 997.

[52] *See* OECD, *supra* note 1, at 57–58; Evans & Noel, *supra* note 8, at 680–83; Filistrucchi et al., *supra* note 8, at 296–300; Katz & Sallet, *supra* note 1, at 2150–51.

[53] *See* Filistrucchi et al., *supra* note 8, at 296–300. This justifies defining one-sided relevant markets, as done by the U.S. Supreme Court in both *Times-Picayune Publishing Co. v. United States* and *Lorain Journal Co. v. United States*. Times-Picayune Publ'g Co. v. United States, 345 U.S. 594, 610 (1953); Lorain Journal Co. v. United States, 342 U.S. 143, 150–53 (1951). The majority also made the same point in *Ohio v. American Express Co.*, 138 S. Ct. 2274, 2285–86 (2018).

Multi-sided platforms can be separated into two categories— *transaction* and *non-transaction* businesses. Transaction platforms are those where buyers and sellers must be joined simultaneously for an observable transaction to occur (observable exactly because it occurs simultaneously).[54] A transaction requires the matching between users on both sides, usually at a rate of 1:1 (i.e., one buyer to one seller). On the other hand, non-transaction platforms still match two or more distinct groups but do not require immediate and observable transactions. For this reason, per usage fees are more common in transaction platforms than in non-transaction platforms (who usually focus on charging membership or access fees).[55]

Because of these distinctions, many authors have asserted that transaction platforms should *always* be defined as a single two-sided relevant market for antitrust purposes. Indeed, in one of the most influential papers analyzing this matter, Filistrucchi et al. assert that "[i]n two-sided transaction markets, only one [relevant] market should be defined."[56] Others have followed suit, equally defending that transaction platforms should be deemed a single multi-sided relevant market for the purposes of antitrust enforcement.[57] More importantly, the *Amex* majority accepted

---

[54] *Amex*, 138 S. Ct. at 2277; Filistrucchi et al., *supra* note 8, at 298; Joshua D. Wright & John M. Yun, Ohio v. American Express*: Implications for Non-Transaction Multisided Platforms*, CPI ANTITRUST CHRON., June 2019, at 5. Marketplaces (e.g., Amazon or eBay), transport network companies (TNC) (e.g., Uber), and payment card networks (e.g., Visa or Mastercard) are all examples of transaction platforms. In marketplaces, the product sold is a transaction between sellers and buyers; in TNCs, the product sold is a ride between drivers and riders; in payment card networks, the product sold is a transaction between a cardholder and a merchant.

[55] Newspapers are the prime examples. When advertisers buy advertising space they cannot be sure when or if customers have seen the ad. This requires newspapers to charge for membership (placing the ad), not for transaction (customer seeing the ad). *See* Filistrucchi et al., *supra* note 8, at 298–99. Credit card networks, on the other hand, organize discount rates that reflect the specific value of the transaction they process.

[56] *Id.* at 302.

[57] Evans & Noel, *supra* note 49, at 674; Klein et al., *supra* note 18, at 580. The OECD also prepared a report on the application of antitrust to multi-sided platforms and invited Filistrucchi to draft the section on market definition, where he again defended that transaction platforms

this literature. Quoting the papers by Filistrucchi, Klein, and Evans, the Court accepted, at face value, that the characteristics of two-sided transaction platforms *always* mandated the definition of a single relevant market, not allowing for discussions about possible one sided-markets within these platforms.[58]

This article proposes an alternative approach that also relies on the theoretical literature on multi-sided markets but that yields somewhat different results from the definitive position stated by the majority opinion in *Amex*. While it is not the first attempt to discuss or challenge the proposition that transaction platforms *always* require the definition of a single two-sided relevant market adopted in the abovementioned literature or in the *Amex* opinion (with Katz and Sallet being the main exponents),[59] it is unique in proposing a framework that separates multi-sided

---

should be defined as a single relevant market. OECD, *supra* note 1, at 42. *See also* Wismer and Rasek's contribution to OECD, *supra* note 1, at 58.
An interesting paper is that of Eric Emch & T. Scott Thompson, *Market Definition and Market Power in Payment Card Networks*, 5 REV. NETWORK ECON. 45 (2006). While they initially focus on network services, ignoring how intra-platform balancing may impact the different sides of the network, they later expand their model to explain how in determinate circumstances the network may ignore one-side of the market and exert market power solely on the other side. This would justify an analysis of the conduct based solely on the side that was subject to the increased prices by the platform. Nonetheless, they focus on inter-network competition for each side of the platform and how networks can extract more profits without impacting the overall platform demand—falling short of the analysis proposed herein on the incentives for players acting in each side of the market. See, however, Hesse and Soven, *supra* note 48, at 728 (defending the use of a SSNIP test on both sides of the payment network in order to define separate relevant markets).

[58] *Amex*, 138 S. Ct. at 2287. One has to point out, equally, that the minority's narrow definition of relevant market as "payment card services to merchants" ignores much of the theoretical literature described above and disregards how network effects may be a powerful competitive constraint, affecting relevant market definition.

[59] Among the most notable papers discussing the subject, see Dennis W. Carlton, *The Anticompetitive Effects of Vertical Most-Favored-Nation Restraints and the Error of* Amex, 2019 COLUM. BUS. L. REV. 93, 103–05 (2019) (criticizing United States v. Am. Express Co., 838 F.3d 179 (2016) and proposing that multi-sided markets be treated like regular one-sided markets where players balance prices and promotions). *See also* Wright & Yun, *supra* note 45, at 721 (broadly agreeing with the *Amex* framework); Patrick R. Ward, *Testing for Multisided Platform*

markets according to how platforms structure the intensity of indirect network effects that characterizes them.

All in all, this article agrees with the literature's conclusions that indirect network effects can run both ways or only one way—i.e., it accepts that the framework established by Filistrucchi and others is largely correct and an useful benchmark. What that framework misses, however, is that there are more circumstances of one-sided network effects (or simply weaker two-sided network effects) than now acknowledged. Our proposed analysis brings a more nuanced and complete approach, allowing for definitions of one-sided markets even within transaction platforms. That is the core of the next part.

III. A MULTI-LAYERED APPROACH TO IDENTIFY ONE-SIDED AND TWO-SIDED RELEVANT MARKETS IN TRANSACTION PLATFORMS

Just because transaction platforms *may* require the definition of a single two-sided relevant market does not mean they *always* require this conclusion, nor that this should be the *only* relevant market for competition law purposes when evaluating a particular conduct or merger. Indeed, there may be single-sided relevant markets within two-sided transaction platforms, their existence depending on the design and structure of these platforms and the amount of intra-platform competition they allow, among other features. In fact, even transaction platforms may comprise more than one relevant market (multiple "layers of competition").

As seen in Part II above, it is well established that the key element leading to the definition of a single two-sided relevant market in a transaction platform is the strength of the network effects

Effects in Antitrust Market Definition, U. CHI. L. REV. 2059, 2089–2101 (2017) (using electronic payments to develop a two stages test when defining relevant markets).

between distinct sides. When network effects are strong, they constrain a firm's competitive conduct in one side of the market, requiring the analysis to simultaneously take into account the different sides. In other words, "[t]he nature and strength of the cross-platform network effects is therefore more important to the analysis than the category of platform [classifying the platform as transaction or non-transaction]."[60] The degree to which one side constrains the other side of the market, however, is an empirical issue that must be evaluated case by case. This may ultimately lead to a "looser form of market definition,"[61] one focused on the intensity of constraints imposed on platforms by network effects.[62]

This foundational insight, however, is often forgotten in the analysis of transaction platforms, as illustrated by the majority's opinion in *Amex*.[63] Some courts and scholars apparently presume that these types of platforms *always* encompass strong network effects.[64] This is a one-dimensional analysis that discards the possibility of different dimensions of competition in a complex platform co-existing. In doing so, the scholarship and *Amex* prevent companies and lower

[60] OECD, *supra* note 1, at 11.
[61] Evans & Noel, *supra* note 8, at 697.
[62] Renato Nazzini, *Online Platforms and Antitrust: Where Do We Go from Here?*, 5 ITALIAN ANTITRUST REV., no. 1, 2018, at 5, 15.
[63] The majority opinion of the U.S. Supreme Court uses very broad language when defining the relevant market in the case: "Evaluating both sides of a two-sided transaction platform is also necessary to accurately assess competition. Only other two-sided platforms can compete with a two-sided platform for transactions . . . Thus, competition cannot be accurately assessed by looking at only one side of the platform in isolation." *Amex*, 138 S. Ct at 2287.
[64] *See supra* Part II. Also, despite Evans's earlier defense of an empirical approach to assess the intensity of network effects, David Evans and Richard Schmalensee were key advocates for a strong presumption in their amicus brief to the U.S. Supreme Court: "For platforms that provide two groups of customers with a service that they must consume jointly, and where the challenged conduct necessarily affects both types of customers, there is a strong presumption that, as a matter of economics, the rule of reason analysis, at the first stage, should consider the impact of the challenged conduct on both groups of customers." Brief for *Amici Curiae* Prof. David S. Evans and Prof. Richard Schmalensee in Support of Respondents at 16, Ohio v. Am. Express Co., 138 S. Ct. 2274, 2285–86 (2018) (No. 16-1454).

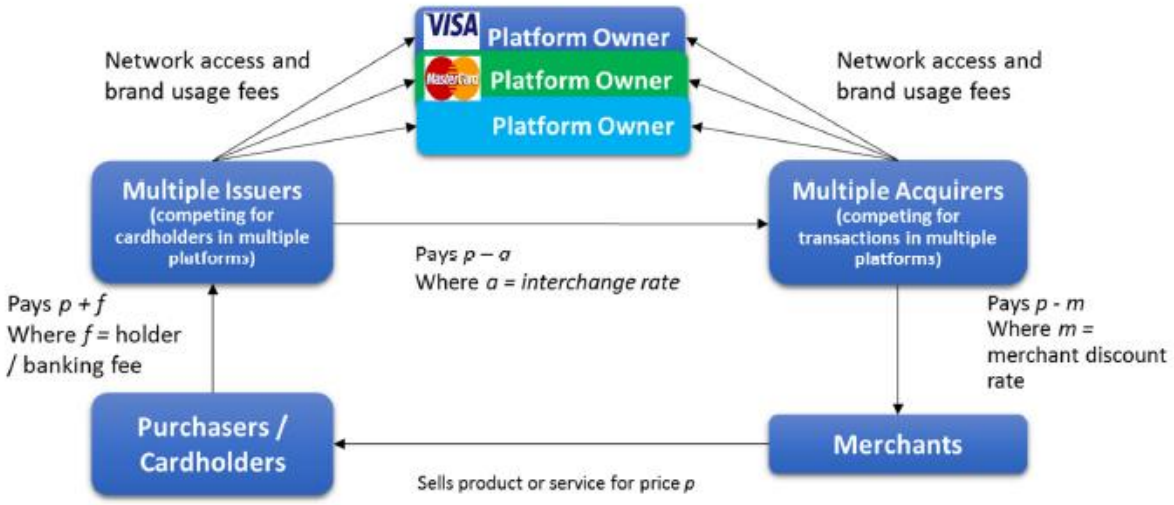
courts from clearly separating the cases where *Amex* and similar frameworks are ruling precedents from those where they are not. The remainder of this part challenges this presumption. While acknowledging that this is largely an empirical, case-by-case matter, any analysis of transaction platforms should consider the multiple dimensions of competition (within and across platforms) and assess to what extent one or multiple sides effectively constrain the different groups of agents that interact to offer particular services or goods. The proper comprehension of these dynamics should help scholar and practitioners alike.

Some complex transaction platforms are structured in ways that allow for multiple spaces of intra and inter-platform competition. In these cases, relevant market definition requires an assessment of whether intra-platform network effects are sufficiently strong to create the type of competitive constraint that demands a single two-sided relevant market. In activities where network effects are weak, there is little reason to define the entire platform as a single relevant market, even when it balances different sides to increase profitability. This is the typical example of newspapers, as discussed above.

There is no reason why a similar rationale should not apply for transaction platforms as well, if and when these platforms create "layers of competition" that are relatively insulated from network effects. For instance, whenever a platform owner allows (or stimulates) competition by firms that act exclusively (or primarily) in one side of the market, these firms may be substantially indifferent to inputs coming from the other side. In these cases, despite being part of a two-sided transaction platform, firms acting solely in one side may be sufficiently isolated, making competitive decisions that are unconstrained by the other side. These weaker network effects can lead to the definition of single-sided relevant markets within transaction platforms.

A more in-depth look at the economic structure created by open four-party payment card platforms, such as Visa or Mastercard may help clarify this discussion.[65] As described in Figure 1 below, these platforms are particularly complex, involving at least five different groups: (1) the platform owner, who is responsible for the payments network; (2) the group of issuers (responsible for offering cards to cardholders), usually composed of different issuing banks; (3) the group of acquirers (responsible for capturing and processing transactions), which may be composed of acquiring banks, independent acquirers (non-banks), or a mixture of both; (4) the cardholders; and (5) the merchants.

FIGURE 2.1: FOUR-PARTY PAYMENT PLATFORMS



In such a payments network, platform owners usually allow for competition among issuers of their branded cards and among acquirers of transactions from these same cards. Therefore, in

[65] Typically, four-party systems, such as Visa and Mastercard, allow for competition among issuers and acquirers in their platforms. Issuing banks compete for cardholders, with different fees, different rewards programs and different premium services. Acquirers compete for merchant transactions, offering different fees (MDR; merchant discount rates) and related financial services. For a general description of the four-party system used by Visa Europe, see *Interchange Fees*, VISA EUR. For a historical take on the formation of both three and four-party systems, see Baxter, *supra* note 1, at 572–82.

these platforms there are at least three potential areas of competition: (1) competition among issuers (e.g., issuing bank A v. issuing bank B); (2) competition among acquirers (e.g., acquirer C v. acquirer D); and (3) competition among platforms (e.g., Visa v. Mastercard v. other Four-Party Systems v. Three-Party Systems[66]). Following the rationale above, differentiating between a single two-sided relevant market and multiple single-sided markets requires evaluating the strength of the indirect network effects in each of these areas of competition to establish whether such network effects pose sufficient constraints on different groups of players. Although this is largely an empirical issue, a general discussion can illustrate the point.

Issuers. First, consider the issuers' group. Issuing banks compete and differentiate themselves through the fees and interest rates they charge to cardholders, rewards programs (e.g., points and airline mileage), and other services and perks offered to cardholders (e.g., access to VIP lounges and concierge services). This leads to inter-brand competition, as issuers of different brands attempt to attract cardholders to their different payments networks. At the same time, there is significant intra-brand competition, as multiple Visa bank-issuers compete for cardholders

[66] Three-party systems are those in which the issuer is also the acquirer of the transaction, establishing direct contracts with both cardholders and merchants (e.g., American Express, Diners, and private labels issued by retail chains). These systems do not require interchange fees/rates and they are usually closed to intra-platform competition, as there is a single issuer and acquirer, which may be the platform owner or a third party licensed by the platform owner. Over the years, some three-party systems like American Express evolved to allow some intra-platform competition, for example, opening part of the system to issuing banks or acquirers (as is the case with the American Express OptBlue program in the United States). Three-party systems and four-party systems compete at the platform level, with different value propositions to cardholders and merchants. For a comparison between four-party and three-party models in electronic payment systems see OECD, COMPETITION AND EFFICIENT USAGE OF PAYMENT CARDS (2006), www.oecd.org/daf/competition/abuse/39531653.pdf.

within the Visa payments network. Finally, banks may multi-home, issuing cards from different brands (i.e., banks frequently issue cards from Visa and Mastercard).[67]

This competition among issuing banks is important in and of itself and, in certain circumstances, should be deemed a standalone relevant market. The design of the transaction platform may reduce the relative strength of network externalities affecting issuers, especially if the issuers are not present on the acquirer side. Indeed, when the primary competition constraint on issuers is the competition from other issuers and not the acceptability of cards on the other side of the platform, the dynamics of competition is closer to a one-sided market. After an issuer joins a specific platform such as Visa or Mastercard, it will compete for each cardholder.[68] In doing so, it takes the other side of the platform—the acceptability of cards by merchants—largely as a given. Marginal variations on acceptance levels have limited impact on issuance decisions and vice-versa. Balancing the platform is simply not in the issuer's hands, but in the hands of the platform owner.

In other words, issuers first make a binary decision on whether or not to join a platform. Then these banks compete among themselves for cardholders within the platforms they decided to join. The relevance of this "competition space" is the reason why an agreement among issuers regarding a competitive variable (e.g., to reduce the ratio dollar/points in a reward programs or to hinder other banks from joining the network, as seen in Europe)[69] would usually raise legitimate concerns for antitrust authorities. This is not to say that network effects are nonexistent, nor that

[67] See, for example, Citibank offering predominantly Mastercard but also Visa cards as part of its services. *View and Compare All Credit Cards*, CITI, www.citi.com/credit-cards/compare/view-all-credit-cards?intc=megamenu~creditcards~vac. In its advertising, Citibank barely mentions that Citi Double Cash or Citi ThankYou cards are a Mastercard. The focus is on rewards, transfer rates, and annual fees.

[68] This assumes the issuer has freedom to establish its prices and conditions of issuance.

[69] *See* Cases C-67/13 P, Groupement des Cartes Bancaires (*CB*) v. Comm'n, ECLI:EU:C:2014:2204 (CJ Sept. 11, 2014); Case T-491/07 RENV; Groupement des Cartes Bancaires (*CB*) v. Comm'n, ECLI:EU:T:2016:379 (GC June 30, 2016).

they do not impact other agents in the market such as platform owners, but rather that the system is designed in a way that these effects are weaker on issuers, not posing significant competitive constraints to the services they deliver on their side of the platform. For this reason, in circumstances such as the ones described above, it may be reasonable to consider the issuer side as a one-sided market within a larger transaction platform.

Acquirers. Somewhat similar dynamics take place on the acquirer side of the platform. Acquirers are the intermediaries that capture the transaction on behalf of the merchant and require authorization from issuers to complete the sale, charging a fee from merchants to perform this service (i.e., Merchant Discount Rate (MDR)). Some acquirers provide the network services to authorize a transaction and ensure that it is implemented. Others hire network providers to perform the operational role of capturing the transaction, while retaining the commercial role of handling the transaction charges and payments.

Acquirers may be more or less vertically integrated to the network owner or to issuers. Acquirers competing for merchants is another potential instance of intra-brand competition—companies such as FirstData and FattMerchant dispute merchants' Visa transactions by charging different MDR rates. There is also some inter-brand competition, as acquirers dispute transactions with acquirers from other brands, especially when cardholders multi-home and may choose to use different cards in each transaction. Finally, acquirers also normally multi-home, handling transactions from multiple brands as in the diagram above. In this context, acquirers compete among themselves to offer the best price and quality of service, as well as value-added services to merchants.

Just as in the case of issuers, independent acquirers may be relatively insulated from the indirect network effects coming from the issuing side. Once the acquirer joins a platform, or

multiple platforms, it will take the cards issued and their respective terms largely as a given, simply disputing the preference of merchants to capture as many transactions as possible. The acquirers' offers to merchants do not impact the points offered or fees charged to the cardholder, so the acquirer is usually incapable of influencing the decision of the cardholder to use one or another card. All in all, these circumstances may justify the definition of a single-sided relevant market encompassing only the acquiring side of the platform.[70]

*Platforms***.** Finally, there are platform owners such as Visa and Mastercard. Their economic incentives differ from those of issuers and acquirers in a way that usually justifies the definition of a single relevant market that encompasses all sides of the transaction platform. That is because, as seen in Part II, owners are the ones who appropriate the bulk of the network effects through their fees and, as such, have the strongest economic incentives and constraints to balance all sides of the platform. The platform owners are also the ones who design and control the tools (e.g., network rules, access fees, interchange rates) used to attract members and to stimulate their use of the platform. In fact, by establishing attractive rules, setting optimal interchange rates, and investing in marketing campaigns to strengthen brand awareness, platform owners increase the overall value of the platform to both issuers, cardholders, acquirers and merchants. The structure of the platform can also enhance or diminish the intensity of network effects, increasing or reducing the exposure of one side to another. The more valuable the platform to all parties, the

[70] The action of the UK Payment Systems regulator, in opening a "Market review into the supply of card-acquiring services," seems to take this view, focusing the market inquiry on a single side of the market in order "to ensure that the supply of these services is competitive and works in the interests of merchants, and ultimately consumers." *See* PAYMENT SYS. REGULATOR, MARKET REVIEW INTO THE SUPPLY OF CARD-ACQUIRING SERVICES: DRAFT TERMS OF REFERENCE (2018), www.psr.org.uk/sites/default/files/media/PDF/Cards_terms_of_reference_July_2018_MR18_1.1.pdf.

more the platform itself can appropriate the surplus it generates by charging higher brand usage and network access fees.

In a somewhat paradoxical move, platform owners may even use the fierce competition in each side of the market to enhance the platform value. When issuers are more exposed to competition on their side of the market (and network effects are less relevant to them as competitive constraints), they may actually: (1) expand the cardholder base in a broader and quicker way, as that is their sole focus; and (2) pay more in fees to the owner, to the extent that they are successful in expanding the base of cardholders. This, in turn, makes the platform more attractive to acquirers/merchants. The same is true of acquirers, whose sole focus on expanding card acceptance is indirectly making the platform more attractive to issuers/cardholders, even if they do not directly appropriate these gains. In this sense, the amount of competition introduced in each side of the platform can be part of the strategy of the platform owner to compete with other platforms. Thus, at the level of the platform owners, competitive constraints usually justify a relevant market that is focused on the overall output of the platform: card transactions.

Recognizing the existence of a two-sided relevant market at the platform level does not eliminate the other layers of competition on the issuers' and acquirers' sides. Different firms integrating these platforms may face different competitive constraints as network effects vary.

Taken together, the examples above show how four-party payment card systems may allow for the co-existence of different relevant markets from a competition policy perspective, including one-sided markets either on the issuer or the acquirer side of the platform. Of course, these relevant markets are inter-related. If the platform owner does not manage the platform well (e.g., setting unattractive rules, establishing excessive fees), it may create skewed incentives and unbalance the two sides, driving members away and ultimately failing. Understanding this dynamic is important.

Because of different relative strengths of network effects on the different groups of firms comprising a platform, some agents have incentives to operate as if in a one-sided market while others consider the multi-sided nature of the platform as a whole.[71] Thus, relevant market definition must account for the fact that there may be one-side competition in two-sided transaction platforms.

Both the majority and the minority in *Amex* and an important part of the literature have failed to acknowledge this complexity. The majority is right to consider that in circumstances where indirect externalities are especially strong there must be a single two-sided market, while the minority also has a point that there may be one-sided markets where firms acting in one side are not particularly constrained by the other side. The question then, is how to design a framework that can effectively identify each situation and cope with multiple layers of competition. This is a key consideration: the lack of a cohesive framework increases legal uncertainty and prevents

[71] On this point, the "multi-layered approach" defended in this article differs substantially from the "multiple-markets approach" presented by Katz and Sallet, *supra* note 1. Indeed, the two approaches resemble each other to the extent that Katz and Sallet also recognize the possible co-existence of different competitive dynamics within multi-sided platforms, leading to multiple relevant markets, even in transaction platforms. However, Katz and Sallet's proposal requires the definition of multiple one-sided markets that may interact through platforms. The existence of network effects must be recognized and taken into consideration, but the authors explicitly refuse "collapsing all of a platform's users into a single product market." Katz & Sallet, *supra* note 1, at 2175. In contrast, the "multi-layered approach" proposed in this article recognizes the possibility of defining "single two-sided markets" in transaction platforms whenever the network effects are sufficiently strong so as to present a significant competitive constraint on firms interacting in the market. Indeed, the method proposed in this article aims at contributing not only to the recognition of multiple relevant markets in two-sided platforms, but also to the establishment of the correct criteria to identify when authorities should define a single two-sided market or multiple one sided-markets to evaluate a certain conduct or merger. In another stark difference, this article also recognizes that a single platform may allow for one-sided and two-sided markets functioning simultaneously (i.e., different "competition layers"), as illustrated in the example of four-party card systems.

private parties and lower courts from properly understanding the limits of *Amex* as a hallmark decision.

The next Part draws from the rich international experience on definition of relevant markets in the payment card industry to both exemplify what a more nuanced approach may look like and show how the lack of a coherent framework may decrease legal certainty.

IV. INTERNATIONAL EXPERIENCE: MULTIPLE RELEVANT MARKETS IN PAYMENT CARDS CASES

Part III above does not rest solely on theory. When faced with concrete cases involving the electronic payments market, antitrust authorities and courts around the world affirmed the coexistence of multiple relevant markets within transaction platforms. There are many relevant examples in Europe and Brazil, jurisdictions with sophisticated antitrust regulators.

i. Europe: *Cartes Bancaires* and Other Cases

a. Cartes Bancaires

Arguably, the *Cartes Bancaires* (*CB*) case is for Europe what the *Amex* case is for the United States—the landmark ruling on how antitrust should analyze multi-sided markets. Results, however, are divergent, as the Europeans adopted a more nuanced approach.

CB is a payment platform just like Visa or Mastercard, created in 1967 as an association of six French banks. As the platform grew to include more than 100 members it subdivided into 11 main members and other institutions linked to main members. In order to align the incentives of the platform among issuing banks and acquiring companies, in 2002 the main members encouraged CB to put in place a system meant to penalize certain issuers through the imposition

of three new fees. In a simplified summary: (1) a fee levied on members whose issuing activities were much larger than their acquiring activities; (2) a fee levied on banks that issued too many cards in the years following their joining of the platform; (3) a fee levied on banks which had not been active in issuing cards but suddenly increased their new issuances.[72]

The European Commission quickly took aim at the new provisions, releasing two statements of objections: (1) the first to CB and nine main members alleging that their new rules were a secret anti-competitive agreement whose object was to stifle competition and limit entry; and (2) the second only to CB with similar content. In 2007, the Commission concluded that CB violated Article 81 (now 101) of the Treaty on the Functioning of the European Union (TFEU) as a measure taken by an association of undertakings that had an anticompetitive object (similar to a per se violation in the United States).[73]

Even though CB (the platform) was the defendant, the Commission defined as a relevant market the "issue of payment cards in France" and affirmed that rather than aimed at balancing out the platform,

> [the] anti-competitive object reflects the genuine objectives of those measures, stated by the main members in the course of their preparation, namely the intention to (i) impede competition of new entrants and to penalise them, (ii) to safeguard the main members' revenue and (iii) to limit the price reduction for bank cards.[74]

[72] Case C-67/13 P, Cartes Bancaires v. Comm'n, ¶ 4 (Sept. 11, 2014). Historically, entry at the issuer level is easier than at the acquirer level, which requires more investment in infrastructure and a relationship with merchants rather than simply attracting cardholders through open-ended offers.
[73] Case COMP/D1/38606—Groupement des Cartes Bancaires, Comm'n Decision (Summary), 2009 O.J. (C 183) 7 (Oct. 17, 2007).
[74] Case C-67/13 P, Cartes Bancaires v. Comm'n, ¶ 8.

The decision also nullified the new pricing measures.

CB appealed and the judicial proceeding followed a course somewhat similar to *Amex*. The General Court (GC)[75] affirmed the initial decision. In its appeal to the European Court of Justice (ECJ), CB affirmed that payment systems were two-sided markets and that by treating its new rules as a "by object" violation on the issuer side the Commission and the GC failed to take into consideration the two-sided nature of the platform.[76] The ECJ largely accepted the theoretical underpinnings of this argument. It affirmed that conduct could only be characterized as restrictive "by object" when history has shown that the said conduct reveals a "sufficient degree of harm to competition that it may be found that there is no need to examine their effects."[77] For the ECJ, the GC failed to establish the conduct's restrictive object. In particular, the GC ignored the indirect network effects between the issuing and acquiring side of the payments platform, so that the new structure could have been set to balance the platform.[78] Therefore, it erred in affirming that the relevant market was the issuing of credit cards in France without further analysis. It should have taken into consideration "all relevant aspects—having regard, in particular, to the nature of the services at issue, as well as the real conditions of the functioning and structure of the markets—of the economic or legal context in which that coordination takes place."[79] As a result, the ECJ concluded that the violations could not be considered illegal "by object" and remanded the case

[75] European Commission decisions are subject to appeal before two European courts: the General Court, which is similar to a district court in the United States, where a single judge decides cases, and the Court of Justice of the European Union, the highest Court in Europe, where a panel issues final rulings.
[76] Case C-67/13 P, Cartes Bancaires v. Comm'n, ¶¶ 34–35. This argument mirrors the *Amex* argument, where the district court considered solely the acquiring side of the platform.
[77] *Id.* ¶ 58.
[78] *Id.* ¶¶ 73–75.
[79] *Id.* ¶ 78.

for the GC to reconsider the case under these guidelines.[80] The ECJ would later confirm this is rationale in *Budapest Bank*.[81]

In remand, however, the GC affirmed its original decision on new grounds and convicted CB once more.[82] While acknowledging the need to take into consideration all the relevant economic and legal contexts that structured the market (its two-sided nature),[83] the GC affirmed that the Commission took those aspects into account in its analysis and that it was correct in defining the relevant market as *the issuing of payments cards in France*. For the GC, the two-sided nature of the platform does not necessarily imply that only one relevant market exists—one may find three distinct markets in (1) the issuing of cards, (2) the acquiring of transaction, and (3) the organization of the payment systems as a whole. While there is interdependency in demand, the services offered are different and aimed at different customers, therefore following different economic incentives.[84] According to the General Court, the ECJ *CB* decision required solely that the interdependency between the issuing and acquiring markets is considered in the assessment of the possible anticompetitive effects of the practice.[85] The Commission considered these issues

[80] *Id.* ¶¶ 82–87, 99.
[81] Case C-228/18, Gazdasági Versenyhivatal v Budapest Bank Nyrt. and Others (Apr. 4, 2020). In a rough summary, the case concerned an appeal by seven banks against a decision by the Hungarian Competition Authority considering illegal by object an agreement between the banks and a representative of Visa and Mastercard to establish uniform levels for interchange fees. The ECJ affirmed the rationale of *CB* with regards to the findings of per object infringements in complex markets—authorities must be certain that the conduct has no possible pro-competitive rationale. It also held that payment cards networks comprised three distinct but connected relevant markets, one for the networks, one for card issuing services and one for acquiring services. *Id.* ¶¶ 6-7; 51-54; 56.
C-67/13 P, Cartes Bancaires v. Comm'n, ¶ 4 (Sept. 11, 2014).
[82] Case T-491/07 RENV, Groupement des Cartes Bancaires (*CB*) v. Comm'n, ECLI:EU:T:2016:379 (GC June 30, 2016).
[83] *Id.* ¶¶ 69–71.
[84] *Id.* ¶¶ 77–80.
[85] *Id.* ¶¶ 82–83.

when it concluded, in part through the testimony of other smaller banks, that the restrictions imposed by the new pricing structure greatly restricted entry in the issuing market because the difficulties in entering the acquiring market made the fees hard to avoid. As a result, the measures were not intended to "balance" the platform but to protect issuing banks from competition.[86]

The *CB* decision exemplifies how an authority may consider the different economic incentives that are present within a multi-sided transaction platform when defining relevant markets and assessing potential anticompetitive effects. The GC appears to have correctly recognized that banks used their control over CB to adopt measures aimed mostly at insulating them from competition on the issuers' side rather than balancing the platform. As a four-party scheme, issuing banks on the CB platform were largely shielded from the indirect network effects on the merchant side when offering cards and card-related services to cardholders. According to the GC, this justified looking at the market as one-sided—issuers blocking other issuers from competing—rather than focusing on the platform as a whole. Thus, the view that banks used the internal CB rules to enforce their illegal agreement to limit entry in one side of the market.

Other European cases, however, demonstrate how the lack of a coherent framework increase legal risks when regulators and courts are faced with these complex economic structures. In particular, one can look at the different decisions reached in the *Mastercard* and *Visa* cases where relevant markets were defined at the platform level, the issuer and the acquirer level without much consistency to exemplify the need for the multi-layered approach proposed herein.

[86] *Id.* ¶¶ 84–85, 92.

b. Visa[87]

In *Visa* the Commission investigated whether the imposition of non-discrimination rules and the definition of interchange fees by Visa violated Article 81 of the TFEU. The Commission defined two relevant markets affected by the practices: (1) one for financial institutions rendering card-related services (issuance of cards and acquisition of transactions); and (2) one for payments systems (the payments network).[88] On the material assessment, the Commission analyzed in detail how the practice impacted both inter-system competition and intra-system competition. On the non-discrimination rule, it used empirical evidence to conclude it had no material effect on competition. The Commission also concluded that the interchange fee setting was an agreement that restricted competition between banks. Nonetheless, it recognized that it was not a price-fixing arrangement but rather a way to stabilize demand on different sides of the platform, and so approved it under Article 81(3) as efficiency enhancing.[89] In doing so, it analyzed how the interchange fee impacted competition on all three relevant markets and recognized that it did not rule out competition between issuing banks for cardholders, acquiring banks for merchants, or between payment systems.[90] This case illustrates the co-existence of multiple layers of competition in the payments card industry, also pointing out how a single practice may have different impacts in each layer.

[87] Case COMP/29.373, Visa Int'l—Multilateral Interchange Fee, Comm'n Decision, 2002 O.J. (L 318) 17 (July 24, 2002) (no longer in force; date of end of validity 12/31/2007).
[88] *Id.* ¶ 43. However, it left the specific relevant market definition open because it found no material adverse effects from the practices.
[89] *Id.* ¶ 69; T-491/07 RENV, Groupement des Cartes Bancaires (*CB*) v. Comm'n, ¶¶ 94–95.
[90] Case COMP/29.373, Visa Int'l—Multilateral Interchange Fee, ¶ 106.

c. Mastercard/Visa Europe[91]

The Commission changed its approach when analyzing the setting of intra-EEA and SEPA fall-back interchange fees by Mastercard in Mastercard and Maestro consumer transactions. Although economic incentives seem similar in both cases, the Commission explicitly ruled out the existence of a single two-sided market when analyzing Mastercard's behavior. Arguing that the setting of interchange fees restricted mostly intra-system competition, the Commission defined two distinct relevant markets for issuers and acquirers' services, and affirmed that they interacted.[92] It ultimately analyzed the conducts' impact on card acquiring services[93] and affirmed that Mastercard did not present sufficient evidence to prove that the fixing of fallback interchange fees was necessary to balance out the platform—forbidding the company from setting minimum fees.[94] The ECJ upheld the decision.[95] There was no discussion on the constraints caused by indirect network effects coming from the issuer's side of the platform. The Commission followed a similar rationale in *Visa Europe*, when it had the opportunity to reaffirm its single-sided market definition as late as 2019, which was after the *CB* decision.[96]

[91] Joined Cases COMP/34.579—MasterCard & Case COMP/36.518, EuroCommerce & Case COMP/38.580—Commercial Cards, Comm'n Decision (Dec. 19, 2007) (*EU Mastercard Cases*); Case COMP/39.398—Visa MIF, Comm'n Decision (Aug. 12, 2010).
[92] *EU Mastercard Cases*, ¶¶ 261–265; 273–274.
[93] *Id.* ¶ 307.
[94] *Id.* ¶ 759.
[95] *See* C-382/12 P, MasterCard v. Comm'n, ECLI:EU:C:2014:2201.
[96] Case COMP/39.398—Visa MIF, ¶¶ 13–16 (separating the upstream network market (inter-platform competition) from downstream "issuing" and "acquiring" markets and affirming that the setting of the interchange fees for debit and credit transactions impacted mostly the downstream market for acquiring services). Visa ultimately settled the case. *See* Case AT/39.398—Visa MIF, Comm'n Decision ¶ 22 (Apr. 29, 2019) (confirming the new commitments decision issued on November 26, 2018, ec.europa.eu/competition/antitrust/cases/dec_docs/39398/39398_14155_4.pdf).

d. Mastercard UK[97]

The former Office of Fair Trading adopted a somewhat similar position when investigating Mastercard's interchange fees in the UK. The OFT defined three distinct relevant markets: (1) a wholesale market between issuers and acquirers for the completion of Mastercard transactions; (2) a Mastercard issuing market; and (3) a Mastercard acquiring market.[98] In doing so, the OFT expressly rejected the existence of a single two-sided market. The OFT found that by fixing interchange fees Mastercard violated Article 81(1) of the TFEU by restricting competition in both the wholesale and the acquiring markets.[99] It also said that to the extent that the interchange fees reimbursed acquirers for services to cardholders, such as loyalty programs, it was an illegal transfer of resources from merchants to issuing banks and some cardholders—another violation of Article 81(1) TFEU.[100]

e. Overview

The cases noted above show how European authorities and courts are inconsistently defining different relevant markets within transaction platforms. While the definition of different relevant markets is generally aligned with the multi-layered approach proposed in Part III, not all of the decisions above are aligned with the framework proposed herein. The Commission and the OFT failed to recognize the important differences between the economic incentives of all the parties that comprise the CB, Visa and Mastercard platforms. In particular, Visa and Mastercard incorporate the indirect externalities of the whole payments network, so that the setting of interchange fees are not a cartel-like practice, but rather a reflection of the need to balance between

[97] Case CP/0090/00/S—MasterCard/Europay UK Ltd, Office of Fair Training (OFT), Decision No. CA98/05/05 (Sept. 6, 2005).
[98] *Id.* ¶ 137.
[99] *Id.* ¶¶ 391–393.
[100] *Id.* ¶¶ 678–680.

issuing and acquiring activities. This justifies the adoption of a single multi-sided relevant market, as done by the Commission in Visa I but rejected in the other cases.[101] Such a rejection, however, ignores the inter-platform competition among payment systems and the intrinsic pressure on platform owners to balance all sides in order to generate value. It is the equivalent of arguing that the platform owner operates separately on both sides of the platform, not being constrained by network effects between them—an argument that ignores that Visa and Mastercard are independent companies that do not operate as issuers or acquirers (especially after their IPOs). Without taking a position on whether another definition of relevant market would have changed the outcome of these cases, the point here is that defining a single two-sided relevant market seems more appropriate, better accounting for the constraints coming from network effects.

In *CB*, however, the Commission and the General Court were correct in focusing their analysis on the issuer side of the market. The conduct seemed primarily aimed at this side, and intra-platform competition seemed essential, given the limited inter-platform competition in France.[102] Also, the relative insulation of the issuing side from constraints coming from the acquirer side made it reasonable to define a one-sided market. *CB*, however, also uses broad language to separate multi-sided from one-sided markets. Indeed, while not being the focus of this article, we believe that *CB* is as much in need of a cohesive framework to increase legal certainty as was true in *Amex*.

---

[101] This largely follows the arguments laid out by Filistrucchi et al. indicating the failure of the Commission to recognize the importance of balancing out indirect network effects for the whole payments network. Filistrucchi et al., *supra* note 8, at 310–15.

[102] *See* Case COMP/D1/38606—Groupement des Cartes Bancaires, ¶ 170 (Oct. 17, 2007), ec.europa.eu/competition/antitrust/cases/dec_docs/38606/38606_611_1.pdf ("The weakness of intersystem competition in France increases the need for robust intrasystem competition. In other words, the stronger the position of a system in intersystem competition, the more serious is any weakening of competition inside it.").

ii. Brazil and the Recognition of Multiple Layers of Competition in the Payment Card Industry

The Brazilian Competition Authority—the Administrative Council for Economic Defense (CADE)—has also been active in the electronic payments industry. Over the past decade, CADE concluded more than ten investigations that touched upon different aspects of these platforms and led to the definition of multiple relevant markets in different cases. Noteworthy examples include: (1) Visa-Visanet; (2) Itaú/Credicard; (3) Elo and (4) Stelo.

a. Visa-Visanet

The first relevant investigation is the 2009 *Visa-Visanet* case.[103] This case focused on a long-standing bi-directional exclusive agreement between Visa (the platform owner) and Visanet (the largest acquirer in the Brazilian market—a Brazilian company): Visa guaranteed Visanet exclusivity in acquiring all Visa credit and debit transactions in Brazil. In return, Visanet accepted to work solely with Visa.[104]

CADE defined distinct relevant markets for credit and debit cards, with a potential subdivision according to services. It then challenged this exclusive relationship, arguing it limited competition in the relevant market of "card-acquiring services rendered to merchants."[105] While

[103] Settlement Proposal n.08700.003240/2009-27, Parties: Visa Int'l Serv. Ass'n & Visa do Brasil Empreendimentos Ltda., Fed. Official Gazette (DOU): 01/29/2010 (2010) (related to Administrative Proceeding no. 08012.005328/2009-31). One of the authors, Pereira Neto, counseled Visanet in this case.

[104] Other acquirers also had de facto exclusive relationships: Redecard was the single acquirer for the Mastercard network, and American Express had its own acquiring system. The whole Brazilian system was set up as an inter-brand competition among platforms and among their respective acquirers. Visa and Mastercard, however, had no exclusive agreements on the issuing side and Brazilian banks competed to issue cards and offer different commercial terms to cardholders. Only American Express also restricted the issuance of cards, much in the same way as in the United States.

[105] Settlement Proposal n.08700.003240/2009-27, Visa Int'l Serv. Ass'n, *supra* note 103, at 11.

acknowledging the importance of inter-brand platform competition for transactions, it claimed that multi-brand acquirers would increase competition for merchant transactions. In doing so, CADE implicitly considered that competition among acquirers in that context was relatively insulated from the issuing side of the market. Eventually, Visa and Visanet settled the case and signed a "cease and desist commitment" that opened both the platform and the acquirer markets.[106] This settlement significantly changed the Brazilian electronic payments' market, as the multi-brand acquirer market witnessed the entrance of both new acquirers and new payment systems (including local brands such as Elo, described below).

b. Itaú/Credicard[107]

CADE approved Itaú's (the largest private Brazilian bank) acquisition of Citibank's credit-card issuance operations in Brazil (called Credicard). CADE's review focused on the relevant market for the issuance of credit cards in Brazil, regardless of the brand (Visa, Mastercard, American Express, or others). Following the rationale proposed herein, it argued that issuing banks compete mostly with other issuing banks for cardholders' preference, studying how the transaction impacted competition on the issuer market. It ultimately approved the transaction after it found strong rivalry among issuers (notwithstanding the fact that Itaú controlled 30-40 percent of the issuing market).

[106] *Id*. at 26. The settlement ended the exclusive relationship and required Visa to establish objective criteria and make efforts to license other acquirers in Brazil and Visanet to accept other major card brands.

[107] Merger n.08700.006328/2013-87, Itaú Unibanco S.A., Banco Citibank, Banco Citicard S.A. & Citifinancial Promotora de Negócios e Cobranças, Fed. Official Gazette (DOU): 08/22/2013 (2013).

c. Elo[108]

Under the merger review rules, CADE reviewed a joint venture between Bradesco, Banco do Brasil, and Caixa Econômica Federal (three large Brazilian banks) to create Elo, a competitor to Visa and Mastercard. At launch, Cielo (the new name of Visanet) was Elo's single acquirer. CADE's analysis focused on inter-brand competition among platforms and the vertical relationships between brands, issuers, and acquirers. CADE defined three distinct relevant markets for payment card systems, credit card issuance and acquiring services—studying these separate but interrelated relevant markets. It affirmed that Elo would be procompetitive, spurring rivalry in a payment system market dominated by Visa, Mastercard, and American Express. CADE thus cleared the formation of the joint venture conditioned on the parties' providing "non-discriminatory treatment to other players, especially in the markets for card issuance and acquiring services."[109]

Later, CADE opened an investigation focusing on the exclusive acquiring relationship between Elo and Cielo. Elo signed a "cease and desist commitment," opening its acquiring business to other companies under non-discriminatory provisions so as to promote competition on the acquirer side.[110] Again, CADE defined inter-platform competition between multiple payment systems and the competition among multi-brand acquirers as distinct relevant markets.

[108] Merger n.08012.000332/2011-28, Banco do Brasil S.A., Banco Bradesco S.A., and Caixa Econômica Fed., Fed. Official Gazette (DOU): 12/09/2011 (2011). Both authors counseled Elo in this case.
[109] *Id*. at 599.
[110] Settlement Proposal n.08700.003614/2017-14, Elo Serviços & Elo Participações S.A., Official Gazette (DOU): 07/04/2017 (2017) (related to Proceeding no. 08700.000018/2015-11).

d. Stelo[111]

CADE also analyzed a joint venture between Cielo, Bradesco, and Banco do Brasil to create Stelo, defined as a payment-facilitation company.[112] CADE defined two relevant markets, an upstream market for acquiring services (performed by Cielo) and a downstream market for facilitation services. CADE first analyzed how facilitation companies are at the same time potential competitors and clients of acquiring companies. It then analyzed if Cielo could foreclose the facilitation services on behalf of Stelo and vice-versa. CADE approved the transaction once it found strong competition in both markets.

e. Overview

CADE's experience also demonstrates how multiple layers of competition co-exist within complex transaction platforms such as electronic payment services. While CADE's framework largely follows the multi-layered approach proposed herein, the authority should more seriously consider and evaluate potential constraints coming from network effects in payment platforms. CADE sometimes seems too eager to define multiple one-sided markets. For example, payment facilitation services could be part of acquiring services—indeed, only a couple of years later Cielo incorporated Stelo as a subsidiary, and other payment facilitators became full-blown acquirers. The acknowledgement of multiple layers of competition should not lead to an excessive bias towards the analysis of one-sided markets within platforms.

[111] Merger n.08700.004504/2014-27, Companhia Brasileira de Soluções e Serviços, Cielo S.A. & Stelo S.A., Official Gazette (DOU): 10/01/2014 (2014). Both authors counseled the companies involved in this joint-venture.

[112] Stelo rendered services in between acquirers and merchants. Merchants can hire Stelo to process online payments and provide IT services, in particular cash and inventory management and electronic wallets. Stelo, however, was not part of any payment systems and hired Cielo to process its transactions.

iii. Summary

Authorities around the world have analyzed the competitive dynamics of separate but interdependent relevant markets that co-exist within electronic payment platforms. Such case law, which many times correctly recognized the existence of one-sided markets within multi-sided platforms, would not be possible under the rigid approach proposed by *Amex.*

Still, even in these cases competition authorities seem to miss a framework that explains why, when faced with specific issues, they opted for these independent but interconnected relevant markets or for a single two-sided market. The framework developed in the next part helps provide some guidance on how to proceed in such cases.

V. TOWARDS A FRAMEWORK TO DEFINE RELEVANT MARKETS IN TRANSACTION PLATFORMS

Defining relevant markets is not a goal in and of itself. It is a tool (1) to identify the areas of competition under analysis (including the universe of competitors and customers), (2) to understand the competitive dynamics within that market and, ultimately, (3) to assess the firm's market power. Even when authorities avoid a precise definition of relevant markets, they must have a general understanding of the competitive dynamics in that segment of the market to proceed with the analysis. In fact, relevant markets (whether precisely defined or generally assumed) are the lens through which authorities and courts analyze competition issues.

As Part II shows, multi-sided platforms present strong network effects, which may impose additional competitive constraints on firms that need to balance out platform participation. This may lead to multiple layers of competition and require the definition of multiple relevant markets, depending on the actual competitive constraints faced by the different firms that are part of a given

platform. Identifying these different relevant markets, establishing the competitive dynamics in each one of them, and acknowledging eventual relationships among them is crucial for an accurate antitrust analysis. This perspective that focuses on the multiple market segments where firms compete within and across platforms is the "multi-layered approach" referred to in the title of the article.

A key issue in implementing this approach is to develop a framework that allows for the identification of which layers of competition may be important for the analysis, and whether these layers imply one-sided or two-sided relevant markets. As the examples from the payment card industry show, the intensity of network effects (and the consequent feedback loop that comes from other sides of the platform) may vary significantly and may affect different firms operating in these platforms in different ways. Thus, any framework to define relevant markets in these platforms should be structured to identify and take these variations into account, something that is missing in the current approaches to this problem.[113] The lack of a coherent framework is problematic because it increases legal uncertainty and hinders the enforcement of an effective antitrust policy.

This Part draws from the literature review, the insights explained in Part III,[114] and the examples discussed in Part IV to propose a more general and somewhat still easily applicable framework to help define relevant markets in multi-sided transaction platforms. Overall, it

[113] Katz and Sallet's "multiple-markets approach" is the most important contribution to date. While it acknowledges the possibility of more than one relevant market in these platforms, it does not present a framework to define whether these markets are one-sided or two-sided. They always seem to rely on the definition of one-sided markets (looking at substitute products for each group of users), leaving the question of whether constraints come from another side to the assessment of market power and effects on competition. In our view, even though their proposal makes an important contribution to the literature, it is insufficient to fully capture the different competitive dynamics in transaction platforms. *See* Katz & Sallet, *supra* note 1.

[114] That two-sided transaction platforms may have multiple layers of competition, requiring the definition of multiple relevant markets—depending on the actual competitive constrains on the firms involved.

advocates a four-step process that enables antitrust authorities and courts to properly assess the economic incentives at play within a multi-sided business model, helping them define one or more relevant markets as impacted by a given conduct/merger. These steps are: (1) evaluate the structure of the platform and the existing "competition spaces", or the segments of the market where firms interact; (2) define a preliminary relevant market (usually a one-sided market), focusing on the competition spaces primarily affected by the merger or conduct under scrutiny; (3) consider multi-sided constraints to potentially expand this definition to include different sides in a single relevant market; and, finally (4.a) define the boundaries of a multi-sided market, or (4.b) define the boundaries of a one-sided market. These steps are more fully outlined below.

i. The Four-Step Process to Define Relevant Markets

1. Evaluate the structure of the platform. First, authorities must evaluate the structure of the platforms competing to supply a given transaction (e.g., payment; sale of a good; sale of service) and identify whether and where they enable/encourage intra-platform competition, inter-platform competition, or both. This means mapping out the different economic activities that compose or that are directly connected to the platform under analysis.

Payment card networks, for example, may simultaneously allow for both inter-platform competition (e.g., among card brands) and intra-platform competition (e.g., among issuers or acquirers of the same brand). This first step then means mapping these initial competition spaces where different firms compete over the preferences of one or multiple groups of platform users—merchants, cardholders, issuing and acquiring banks, and other payment networks in the example of payment cards, but also buyers, sellers, advertisers, and other platforms in the example of marketplaces. These competition spaces are not yet relevant markets for competition law

purposes, but are a first step that allows authorities to grasp the full picture of the competitive dynamics within and across platforms impacted by a given conduct or merger.

2. Define a preliminary relevant market (focusing on one-sided markets). Second, authorities should initially focus on the specific, one-sided "competition space" most affected by the merger or conduct under scrutiny. If the conduct disproportionally impacts a given group of intra-platform users, this will be deemed a preliminary "competition space" and the analysis should start by assessing that side of the platform. Usually, the starting point will be a single-sided market, affecting one group of users. For example, in a merger between issuing banks not active on the acquirer market, this preliminary relevant market should be the issuers' side of the platform.

Authorities must then scrutinize the competitive dynamics on this specific side, not yet considering potential two- or multi-sided constraints.

First, they should check whether the platform itself is designed in a way that promotes/encourages intra-platform competition on that side of the market (i.e., multiple players in the same side of the market) and/or inter-platform competition (i.e., the products or services offered in other platforms that might be considered close substitutes for that particular group of users). Strong intra-platform competition is an indicator that this preliminary one-sided market may be relevant in and of itself, while strong inter-platform competition may indicate other connected markets or the presence of a multi-sided relevant market. Keeping the same example, an issuer of a Visa card competes with other issuers of Visa cards (intra-brand competition) and issuers of cards from other brands (inter-brand competition)—potentially two different markets. American Express mostly issues its own cards (no intra-platform competition), so the focus is on inter-platform competition with other payment card networks like Visa and Mastercard.

Second, authorities must also check for the presence of multi-homing, or if groups of users usually access a single platform or multiple platforms. This is relevant to define whether there is only one dimension of competition at the adoption/membership level (i.e., in the absence of multi-homing, users simply decide whether to adopt platform A or B) or if there is competition at the transaction level as well (i.e., in the presence of multi-homing, users may adopt multiple platforms and make a decision on what platform to use in each transaction). This analysis is still focused on one side of the platform, looking from the perspective of the user on that side (e.g., merchants in the acquirer side and cardholders on the issuers side) and it is aimed at identifying whether there is a single dimension of competition (i.e., adoption) or two dimensions (i.e., adoption and use). When multi-homing is widespread and there is fierce competition for preferences at the use level, use should be the primary focus of the analysis.[115]

3. Consider potential multi-sided constraints and define one-sided or multi-sided markets. Third, once authorities identify the competitive constraints on one side of the market and define one (or, in case necessary, multiple) preliminary relevant markets, they must then assess whether constraints posed by the other side(s) of the platform are relevant enough to influence the

[115] Filistrucchi et al. argue that it would be necessary to define two relevant markets, one for adoption and one for use. Filistrucchi et al., *supra* note 8, at 312–13. Although competition for use poses an additional competitive constraint on firms, it does not necessarily lead to separate relevant markets. First, when multi-homing is widespread, adoption tends to be easy and costs tend to be low, diminishing the relevance of adoption as a competitive variable. Indeed, in this context, even if users single-home, they have potential easy access to other platforms. Second, even if users multi-home in adoption, they may (and usually do) concentrate use in one platform (i.e., prefer a particular card brand). In these contexts of intense multi-homing, the focus should be primarily in use. In contrast, in single-homing markets, competition for adoption tends to be more important. Overall, looking at single- and multi-homing as a way to identify whether the focus of analysis should be on adoption or use (instead of always defining two relevant markets) tends to simplify an already complex analysis.

strategic behavior of the players under scrutiny—something that justifies abandoning the preliminary one-sided definition and moving to a two-sided market.

This is the crucial step in market definition. In most cases, this decision for one- or two-sided markets will depend on the following aspects:

1. The structure of the platform and its internal rules—e.g., whether it allows for intra-platform competition or not;
2. Whether the players under scrutiny have any control over how the platform balances indirect externalities or if they simply take them as a given (i.e., whether the players under analysis internalize these externalities and reap the benefits of the growing value of the platform for multiple users);[116] and, most importantly
3. The strength of indirect network externalities (i.e., the degree of interdependence of demand on both sides and the intensity of the feedback loop between them).

When network effects are intense, the firms under scrutiny are particularly exposed to them *and* they have some control over variables that may affect such externalities, it is reasonable to assume that firms' consider more than one side of the platform in their competitive strategies. This justifies the single, multi-sided market definition.

Regulators and parties can assess these three factors through a combination of quantitative and qualitative methods. A review of the internal rules of the platform and of the degree of control over these rules by the different players are necessarily qualitative. In theory, the strength of

[116] For example, in payment card systems, the network owner is usually the one in the best position to internalize externalities, capturing the added value of the network. When the owner is also an issuer (e.g., American Express), it is likely to be more constrained by actions in the acquirer side than when the issuer is not a network owner (e.g., issuing banks in the Visa or Mastercard system).

networks effects may be measured through econometric studies that document whether the platform faces significantly higher price elasticities vis-à-vis what would be expected in similar one-sided markets—indicating the existence of the bandwagon effects that define multi-sided markets. Assessing the intensity of these indirect network effects through quantitative analysis and econometric studies, however, requires hard- to-obtain detailed price and demand data about different markets, making such exercise extremely difficult if not entirely unfeasible in most cases.[117] If this is the case, rather than relying on assumptions and overbroad presumptions about market behavior,[118] regulators and parties can look for four important types of indirect, qualitative evidence on an undertaking's behavior that can help demonstrate strong exposure to indirect network effects and separate single- from multi-sided relevant markets:

1. The undertaking should be able to control or at least directly influence prices on both sides of the platform (set the price structure of the platform, or at least floors or ceilings on different sides).
2. The undertaking should be able to prevent arbitrage between the different sides of the platform (this is usually associated with control over the rules of the platform to prevent the price structure from being undermined by players on either side).

[117] This may change in the future as more data and increased price discrimination allow economists to better map demand curves. *See, e.g.*, Peter Cohen et al., *Using Big Data to Estimate Consumer Surplus: The Case of Uber* 2 (Nat'l Bureau of Econ. Research, Working Paper No. 22627, 2016) (using "remarkable richness of the data generated by Uber" to better define a demand curve and calculate elasticity and consumer surplus).

[118] Indeed, this seems to be a reason why many parties advocated a strong presumption that transaction platforms are a single multi-sided market. *See, e.g.*, Filistrucchi et al., *supra* note 8, at 301–04.

3. The undertaking should be more exposed to inter-platform competition than to intra-platform competition (and, here, the existence of intense multi-homing may be considered evidence of inter-platform competition).

4. The undertaking should derive profits in a relevant manner from revenues/fees collected from the surplus generated by all groups of users rather than profits derived mostly from margins on acquisition and resale to a single group of users (i.e., the undertaking internalizes the externalities generated through intermediation fees that may be charged on both sides or on a single side).

If all or most of the four items above hold true and the undertaking has some control over the rules of the platform, then regulators and parties have a strong indication that indirect network effects are intense and that the undertaking is directly exposed to them. This justifies abandoning the preliminary one-sided market definition in favor of a two-sided relevant market, as this updated definition will provide the best lenses with which to evaluate the competitive impacts of the merger or the conduct under scrutiny. On the other hand, the lack of these features indicates that either network effects are not intense or that the firms under scrutiny are not particularly exposed to them, justifying the confirmation of the preliminary, single-sided relevant market definition established before.[119]

A final question then remains on the extension of these single or multi-sided markets, the concluding steps 4.a and 4.b below.

[119] In this case, indirect evidence of weak exposure to network effects include (1) inability to set or influence in a relevant manner the price structure of the platform; (2) inability to prevent cross-party arbitrage; (3) profits derived mostly from margins on acquisition and resale to a single group of users; (4) exposure to intense intra-platform competition. More generally, evidence that players under scrutiny take action on other sides of the platform as an exogenous input to their own competitive strategies, without relevant influence on these inputs, should reinforce the perception that indirect network effects are weak.

4.a. Define the extension of a single multi-sided market. If the evidence indicates the presence of strong networks effects to justify the definition of a multi-sided relevant market, a final question remains on how to assess the extension of this two-sided market vis-à-vis other potential substitutes.[120] In this case, following Filistrucchi et al., authorities can apply modified econometric tests to assess the boundaries of each market—such as a SSNIP test focusing on price levels (i.e., the sum of the prices charged) and allowing optimal adjustments in the price ratio (i.e., changes in the price structure of the platform).[121] This test allows for a better understanding of whether different platforms are substitutable, identifying the actual competitive constraints faced by the firm when it increases prices and rebalances the price structure at the same time.[122] Such test takes into account the actual constraints on profit maximization of a hypothetical monopolist operating on both sides of the market, leading to the identification of the smallest set of substitute products.

If information is not fully available for a SSNIP test of this kind, a qualitative analysis of substitution may be needed. However, in this type of analysis, product differentiation may pose particularly relevant challenges, as there may be competitive pressure coming from somewhat

[120] For example, in the *Amex* litigation the question was whether credit cards compete with debit cards and/or whether American Express was part of a separate travel and entertainment market of credit cards. *See* United States v. Am. Express Co., 88 F. Supp. 3d 143, 151 (2015).
[121] Filistrucchi et al., *supra* note 8, at 332–33.
[122] This proposition (i.e., applying a SSNIP test focusing on price levels and allowing optimal adjustments in the price ratio), contrasts with that of Evans and Noel, who suggest applying the SSNIP test using a fixed price in one of the sides and a price increase only in the other. *See* Evans & Noel, *supra* note 49. As suggested by Filistrucchi in another paper, the test proposed by Evans and Noel may lead to broader relevant markets than would be appropriate, as the assumption of keeping the price fixed on one of the sides and not allowing it to adjust optimally to the action on the other side, would lead to an overestimation of losses from the price increase, broadening the market definition. *See* Filistrucchi et al., *supra* note 8, at 332 (quoting Lapo Filistrucchi, *A SSNIP Test for Two-Sided Markets: The Case of Media* 11 (NET Inst. Working Paper No. 08-34, 2008), www.ssrn.com/abstract=1287442).

imperfect substitutes.[123] Whether this pressure is sufficient to include these differentiated products in the same relevant market depends on its intensity. Finally, the definition of a multi-sided relevant market for transaction platforms implies that the product under analysis is the number of transactions supported by the platform, and not the specific impacts on a given side of the market. For example, in the case of credit card markets these would be the number of transactions processed by American Express, Visa, or Mastercard; in the case of marketplaces, it would be the number of transactions supplied by sellers to buyers using the platform; in the case of mobility apps it would be the number of rides booked through the platform.

4.b. Define the extension of a one-sided market. If the evidence does not indicate the presence of strong network effects, authorities should then focus on the one-sided relevant market. In this case, it should follow the traditional path of assessing demand- and supply-side substitutability (e.g., SSNIP/critical loss tests, cross-elasticity of demand, price differences),[124] which will usually be sufficient to identify the group of competitors and users in a single side of the market.

Finally, after defining a certain relevant market, authorities should check whether other competition spaces identified in step one might be affected by the same merger or conduct under scrutiny.[125] They should then focus on how the inter-relation between these different relevant

[123] For example, marketplaces may suffer some competitive pressure from price comparison sites and from search engines with vertical searches for retailers.

[124] On how to apply those to a single side of a credit-card market, see Hesse & Soven, *supra* note 48, at 726–28.

[125] For example, as mentioned above, intra-platform competition among issuers of payment cards may have a positive impact on the expansion of the number of cardholders. This, in turn, may increase competition at the platform level for these banks, impacting both a one-sided (i.e., issuers) and a two-sided (i.e., platform) market. Similarly, intense competition among sellers within a marketplace may also contribute to the attractiveness of the platform as a whole, fueling competition among marketplaces.

markets may impact economic incentives of firms. Even if step three rules out the presence of strong indirect network effects and supports the definition of a one-sided relevant market, authorities still must consider how the weak indirect network effects impact firm behavior. In this case, however, these considerations are no longer at the level of relevant market definition but rather when authorities are assessing the firm's market power and its capacity to negatively impact markets or competitors.

ii. Summary of the Framework for Market Definition

The framework proposed above is a more nuanced and more effective approach to market definition than a definition of transaction platforms *always* as (1) a single two-sided market or (2) as multiple one-sided markets with potential defense arguments based on network effects, as argued elsewhere. The first view ignores situations in which firms operating within transaction platforms are not significantly constrained by network effects. The second view fails to acknowledge that, under some circumstances, the intensity of network effects in fact requires an analysis that acknowledges the struggle of platforms to balance the multiple groups they are bringing together. This sharp opposition between two radical approaches to market definition in transaction platforms simply misses the point, leading to a situation in which the tail wags the dog, as a preconceived definition of relevant market applied to all situations drives the analysis, instead of the analysis leading to a sound definition of relevant markets.

The framework proposed in this Part refocuses the analysis on what really matters: the differences in competitive constraints and market dynamics regarding different platforms. Only when these differences are sufficiently strong should they lead to distinctive definitions of relevant markets. Indeed, even the most well-accepted definitions of two-sided markets face important

challenges, and many businesses can adjust their pricing scheme to reflect, at least partly, two-sided market characteristics (e.g., supermarkets).[126]

Antitrust policy should not be based on a framework that leads to a chasm between closely comparable situations. Instead, the framework of analysis should help to identify distinctions that are relevant for applying competition law, also mapping the relevant indirect evidence that may be used to clarify these distinctions. As such, acknowledging the multiple layers of competition in transaction platforms and understanding their interactions is essential to grasp the full complexity of these markets and to perform a sound antitrust analysis.

VI. *AMEX* AND BEYOND: APPLYING THE FRAMEWORK TO TRANSACTION PLATFORMS

This Part uses the approach described above to revisit the *Amex* case and its market definition and show why the application of this framework is important. Then, it moves on to explore market definition in other transaction platforms. The goal is to show that the proposed multi-layered approach applies to other two-sided transaction platforms and not only to payment systems. In doing so, we are more interested in exploring the methodological perspective than actually settling on a precise market definition for each case—a fact-intensive exercise that should always be done on a case-by-case approach.

[126] Katz & Sallet, *supra* note 1, at 2148–51. Think of a supermarket. It can either buy goods and resell at a profit—a normal one-sided business—or it can charge a fee per sale and become a two-sided marketplace. Its antitrust treatment should not differ greatly should it adopt one or another market strategy.

i. The *Amex* Case: Correct Relevant Market Definition and Outcome Given Procedural Limitations but Wrong Guidance

This article has previously argued against the views of the majority and the minority opinions in *Amex*—in particular because of the overbroad language used by Justice Thomas's majority opinion that transaction platforms should always be deemed one relevant market. This view must be better clarified. The *Amex* decision focuses on the definition of relevant markets and on the allocation of burdens of proof. It was the result of a lengthy and extremely costly litigation, including a seven-week bench trial at the district court, where defendants expressly argued that the two-sided relevant market definition was the most appropriate for the case, something refuted by the plaintiffs.[127]

The majority is right in affirming that the correct relevant market is the single multi-sided transaction market and that plaintiffs did not unequivocally meet their burden of proof of demonstrating that the anti-steering clauses damaged competition in the multi-sided credit-card market[128]—something they could have done by demonstrating that higher merchant prices both prevented entry and led to higher prices that were not fully offset by higher cardholder rewards.[129]

[127] United States v. Am. Express Co., 88 F. Supp. 3d 143, 171–72 (2015). Plaintiffs did so apparently relying (in retrospect, wrongly) on the Second Circuit's one-sided market definition in *VISA. See id*. at 172–23 (citing United States v. VISA U.S.A., Inc., 344 F.3d 229, 237, 239 (2d. Cir. 2003)).

[128] Justice Thomas's main reason for ruling in favor of American Express is that "[t]he plaintiffs did not offer any evidence that the price of credit-card transactions was higher than the price one would expect to find in a competitive market." Ohio v. Am. Express Co., 138 S. Ct. 2274, 2288 (2018).

[129] The district court itself, recognized that "as the court has previously noted, neither party has presented a reliable measure of American Express's two-sided price that appropriately accounts for the value or cost of the rewards paid to cardholders." *American Express Co.*, 88 F. Supp. 3d at 215.

We understand[130] that in such lengthy and costly trials American courts are very reluctant to reopen fact-finding under updated guidance from upper Courts, in particular when plaintiffs had a previous opportunity to present the relevant evidence. For this reason, the Court's ruling in favor of American Express appears correct.

Nonetheless, had the Court followed the framework proposed herein and absent any specific procedural limitations, the most correct scenario on that case would probably have been a partial reversal and remand decision, defining a single two-sided relevant market but sending the case back to the district court for further analysis pursuant to the adjusted methodology (as done in other jurisdictions, such as the European Union in the *Cartes Bancaires* decision). More importantly, and as explored at length above, the decision should have provided better guidance to lower courts, private parties, and even to the Supreme Court itself—which surprisingly failed to mention *Amex* when deciding another multi-sided market case, the *Apple Inc. v. Pepper* decision issued in the following term.[131]

a. Relevant Market Definition

Following the framework proposed above, the first step in defining the impacted relevant markets would be to look at the structure of the platform and the existing competition spaces. In the case of payment cards there are at least three levels of competition that normally compose a platform: issuers compete for cardholders, acquirers compete for merchants, and platforms compete for transactions. Second, we should define a preliminary relevant market, focusing on the "competition space" primarily affected by the merger or conduct under scrutiny. In this case,

[130] We are particularly grateful to the experienced U.S. antitrust litigator who served as a referee for this Journal for pointing this out to us.
[131] Apple Inc. v. Pepper, 139 S. Ct. 1514 (2019).

considering that anti-steering clauses were focused on the acquirer-merchant relationship, the primary relevant market would be the acquirer side of the platform.

As a third step, we should look at potential competitive constraints coming from other sides of the market. American Express operates primarily as a three-party vertically integrated payment system,[132] which means both that the platform owner is also the primary issuer and acquirer and that American Express has full control over the design of the platform. As such, there is little room for any intra-platform competition, in sharp contrast to four-party systems where there is competition among multiple issuers and multiple acquirers. Because of this platform structure, constraints coming from the issuer side of the market seem particularly intense, as the company is mostly focused on balancing membership and usage in both sides of the platform (cardholders and merchants).

This is corroborated by the indirect, qualitative evidence indicating strong exposure to indirect network effects referenced above. American Express (1) has the ability to control or at least directly influence prices on both sides of the market (it sets both cardholder rewards, interest rates, and Merchant Discount Rates); (2) has the ability to prevent arbitrage between the different sides of the platform that would undermine the price structure (indeed, that is exactly the goal of the anti-steering clauses); (3) is primarily exposed to inter-platform competition (there is no intra-platform competition, it competes mostly with Visa, Mastercard, and other smaller brands for acceptance and issuance); and (4) appropriates the surplus generated by the platform by charging membership and usage fees to both sides.

[132] We mention "primarily" because in the case of American Express OptBlue and other programs it accepts third-party providers connecting American Express and merchants. *Credit Card Processing for Small Business*, AM. EXPRESS, americanexpress.com/us/merchant/optblue.com.

Based on these characteristics, the Supreme Court seems correct in ruling that American Express operates in a single multi-sided market: the one-sided definition adopted by the district court (and embraced by the dissenting opinion) ignores the important Industrial Organization literature on the topic.[133] Asserting the multi-sided nature is important because only under this framework can American Express properly defend its anti-steering rule as a necessary system to prevent price arbitrage between merchants and customers that would neutralize the effects of the price structure it put in place to balance both sides. More importantly, it allows American Express to argue that it offsets higher merchant fees with higher rewards for cardholders, the core of its two-sided market strategy. The district court erred when it dismissed this balancing by arguing that a harm to one market cannot be compensated by a benefit to a distinct, interrelated market[134]—showcasing the importance of defining a single, two-sided relevant market in this case.

A final, fourth step would then be assessing the boundaries of this two-sided market—whether the relevant market is limited to credit card transactions or whether it should also include debit cards or be restricted in other ways (e.g., focus on travel and entertainment transactions in which American Express is particularly strong). The district court ruling dismissed attempts to expand its relevant market definition to include debit cards or focus solely on the more restricted market for travel and entertainment transactions.[135] For the same reasons referred to by the district court when analyzing a one-sided market, especially the evidence of low cross-elasticity between credit and debit cards,[136] we understand that these boundaries would probably also hold in a two-

[133] *See* Picker, *supra* note 13 (correctly pointing this out).
[134] United States v. Am. Express Co., 88 F. Supp. 3d 143, 229 (E.D.N.Y. 2015).
[135] *Id*. at 170.
[136] *Id*. at 175–76.

sided market of payment card platforms. The court would include in the market other credit card platforms but not include debit cards or focus solely on travel and entertainment.

b. Outcome

In the absence of the procedural limitations noted above, one could argue that the Supreme Court would have erred by not remanding the case to the district court, giving plaintiffs the opportunity to target their arguments to the type of harm required by the Court under the new market definition. That is particularly true because over its long trial the district court gathered relevant evidence that could show harm to competition even under a two-sided market definition, had this been plaintiffs' sole focus.

For example, the District Court found that American Express profitably increased prices over a five year period, which is prima facie evidence of some market power.[137] It also found compelling evidence that the anti-steering clauses, developed to block a successful steering campaign by VISA focused on MDR competition (a campaign that American Express considered "bad" competition),[138] created a negative externality in the market that largely insulated credit-card networks from price competition on the merchant side;[139] led to the increase of MDR rates by Visa and Mastercard who had to issue new high-rewards cards to match American Express' rewards;[140] hindered price transparency and prevented consumers from fully incorporating their

[137] *See id*. at 197, 211–12; Ohio v. Am. Express Co., 138 S. Ct. 2274, 2292–93 (2018) (*Amex*). By definition, market power is the capacity of firms to price above competitive levels, or the ability of firms to influence the market price. A. DOUGLAS MELAMED ET AL., ANTITRUST LAW AND TRADE REGULATION: CASES AND MATERIALS 65–66 (7th ed. 2018). Having market power, however, is not illegal. This prima facie characterization does not necessarily imply an antitrust violation.
[138] *See American Express Co.*, 88 F. Supp. 3d at 211–12.
[139] *Id.* at 209.
[140] *Id.* at 201–02.

cost of using credit-cards;[141] apparently prevented the development of a lower-cost business model by Discover and potentially other entrants;[142] and impeded inter-brand competition amongst card companies, increasing equilibrium prices for all consumers (with a stronger impact in those not holding American Express or other high-rewards cards).[143] Finally, and also importantly, the District Court also found that the anti-steering clauses harmed innovation in the industry.[144]

When combined, these findings deserve further assessment, as they can be important evidence that the anti-steering clauses may negatively affect competition on the merits among the different platforms, potentially leading to increased barriers to entry and higher prices. Indeed, there is growing academic literature explaining how, depending on the circumstances, MFNs and other clauses that similarly weaken price competition may hurt consumers by increasing equilibrium prices and/or excluding competitors[145] and, under different circumstances, such clauses have been condemned in different jurisdictions, including the United States.[146] Professor Dennis Carlton, for example, argues that the specific structure put in place by American Express could harm consumers,[147] and other research has explored how the low bargaining power of

[141] *Id.* at 209.
[142] *Id.* at 213–14; *Amex*, 138 S. Ct. at 2293–94.
[143] *American Express Co.*, 88 F. Supp. 3d at 213–17. This is a particularly negative effect, as it implies perverse regressive cross-subsidies where poorer customers subsidize high-earning customers.
[144] *Id*. at 217–18.
[145] *E.g.*, Jonathan B. Baker & Fiona Scott Morton, *Antitrust Enforcement Against Platform MFNs*, 127 YALE L.J. 2176, 2179–80 (2017); Jonathan B. Baker & Judith A. Chevalier, *The Competitive Consequences of Most-Favored-Nation Provisions*, ANTITRUST, Spring 2013, at 20 (surveying the economic literature on the topic); Carlton & Winter, *supra* note 9 (addressing specifically the American Express clauses).
[146] Baker & Scott Morton, *supra* note 145, at 2186–95 (presenting a survey).
[147] Carlton, *supra* note 59; Carlton & Winter, *supra* note 9.

merchants vis-à-vis large payment networks may lead to higher equilibrium prices that also harm consumers.[148]

As this is a fact-intensive exercise, the majority almost summary, two-page dismissal of this large body of evidence is unconvincing.[149] In the absence of procedural limitations, a fact-finding court would be perfectly capable of re-assessing, under the rule of reason, whether American Express' use of anti-steering rules to implement a business model focused on higher rewards to cardholders offsets the alleged higher prices and increased barriers to entry, or whether a less-restrictive alternative existed.[150]

c. Lack of Guidance

More importantly, however, by accepting at face level the literature on transaction platforms the Court failed in providing lower courts, who will increasingly be faced with similar situations, with proper guidance on when *Amex* should be a considered a binding precedent. Imagine, for example, a situation similar to the *Cartes Bancaires* case in Europe, where issuing banks colluded within a multi-sided platform, another where merchants convene to jointly-negotiate better MDR rates with American Express or even the case against Apple for organizing an e-Book sellers' hub-and-spoke cartel.[151] These are conducts within multi-sided transaction

[148] *See* Vladimir Mukharlyamov & Natasha Sarin, *The Impact of the Durbin Amendment on Banks, Merchants, and Consumers* (Faculty Scholarship at Penn Law, Paper No. 2046, 2019).
[149] Ohio v. Am. Express Co., 138 S. Ct. 2274, 2288–90 (2018) (*Amex*).
[150] This article is focused on market definition and we do not have the necessary information to assess which side would prevail in this new analysis.
[151] United States v. Apple Inc., 952 F. Supp. 2d 638 (2013) (*Apple e-Books*). In the *Apple e-Books* case, prosecutors demonstrated how book publishers had been trying to find a way to increase book prices. Apple then created the agency system which allowed them to do just so. The email exchanges in the case make it clear that Apple required most publishers to be on-board at the same time and imposed the MFN clause as a way to ensure that prices would rise, or at least that it would not lose money against Amazon. Apple therefore was considered to act as a facilitator in a cartel of book publishers to increase prices—not merely as a platform trying to balance both sides (which it would have done by simply setting the 30% agency fee and allowing

platforms so, in theory, the *Amex* framework would apply. Lower courts are at miss on whether *Amex* is the ruling precedent, meaning, for example, that banks or merchants may actually win a U.S.-style *Cartes Bancaires* by claiming there was no impact on credit-card transactions or that Apple was probably correct in claiming it was solely creating a new market for e-books and not organizing a hub-and-spoke collusion.[152]

Perhaps the best way to show this confusion is by looking at the Supreme Court's own precedents. In the following term the Court decided *Apple Inc. v. Pepper*,[153] a case that also involved multi-sided transaction platforms: the Apple App Store marketplace. Surprisingly enough, even after the fierce division of the Court in 2018, neither the majority nor the minority even mention *Amex* as a relevant precedent—despite its clear applicability. An *Amex* decision that followed our framework would have shown how the *Apple Inc. v. Pepper* outcome that consumers can sue Apple is correct (even if the factual description of the majority opinion, that customers buy apps from Apple, is incorrect). Apple, as the platform owner, is in the business of balancing both sides of the market: (i) it has the ability to control or at least directly influence prices on both sides of the market (by fixing fees); (ii) it has the ability to prevent arbitrage between the different sides of the platform that would undermine the price structure (all transactions must be made

---

publishers to join or not the platform at will). This example both exemplifies how both multi-sided (book sale platform) and a single-sided (book publishers) markets may co-exist and the importance of specific circumstances in any given assessment. *See id.* at 647–48.

[152] Indeed, Amex has been invoked by lower courts to help settle concerns around relevant market definition in cases where the two-sided nature of the markets is far from clear. See, for example, Federal Trade Commission v. QUALCOMM INCORPORATED (Court of Appeals, 9th Circuit, 2020) and United States v. Sabre Corp., (D. Del., No. 1:19-cv-01548, Order 4/7/20).

[153] Apple Inc. v. Pepper, 139 S. Ct. 1514 (2019). The case ranged on whether iPhone owners can sue Apple for potential antitrust violations connected to the App Store charging practices or whether only App Developers have this power. The Court struggled to understand who Apple's App Store customers are: the app developers, iPhone owners or both (as a multi-sided analysis would indicate).

through the app store); (iii) it is primarily exposed to inter-platform competition (there is no intra-platform competition within iPhones); and (iv) it appropriates the surplus generated by the platform, mostly through usage fees. Therefore, both app developers and iPhone users are direct "consumers" of the platform and should be capable of bringing a lawsuit alleging potential antitrust infringement under the *Illinois Brick* framework.

By being more structured and well-grounded on the industrial organization literature, allowing for a better distinction between different types of competitive dynamics, the framework proposed herein will allow private parties and lower courts to better understand the boundaries of multi-sided rationale in antitrust assessment. In doing so, it should help increase legal certainty in these ever more important, complex and highly dynamic markets.

ii. Some Insights on Other Transaction Platforms

The framework proposed above to help separate between vertical and horizontal relationships within transaction platforms is not restricted to *Amex* and electronic payments' markets. As the brief example above involving the *Apple Inc. v. Pepper* case shows, it can be applied to many other transaction platforms, including but not limited to marketplaces, property sharing platforms, e-booking platforms, and transport network companies. Each of these platforms is structured differently. They rely on different degrees of openness to intra- and inter-platform competition, something that influences how parties are exposed to indirect network effects. These diverse structures may lead to different relevant markets.

This Part illustrates how the indirect network effects should be taken into consideration in different contexts. One should note that any real analysis is fact-intensive and should start with focusing on the specific merger overlap or the conduct under scrutiny, leading to preliminary

market definition (step two of the framework proposed above). Yet, the summary presented below provides some insights on how to consider indirect network effects in different contexts.

a. Marketplaces

Online marketplaces are clear examples of transaction platforms: matching suppliers and consumers, allowing for observable transactions (sales), and charging mostly per transaction fees. Similar to payment cards, marketplaces such as Amazon, eBay, Jet.com, Etsy, Mercado Livre, App Stores etc. are in the business of bringing together sellers and buyers, a process that generates value to the platform. Therefore, they are constrained by indirect network effects and need to account for both sides of the platform when setting the fees. This may lead to the definition of a single two-sided relevant market from the perspective of the platform owner. Such a relevant market would encompass other platforms that allow transactions between suppliers and customers of goods and services. In the case of pure marketplaces (i.e., platforms in which owners do not act as sellers), network effects seem to be particularly intense, increasing the utility of the platform as the number of buyers and sellers rises.

However, these platforms also host several other competition spaces. From the perspective of sellers in these marketplaces, the number of buyers on the other side is taken as given, and they compete in their side of the platform (i.e., supply of goods and services). For these sellers, just like issuers of payment cards, the key decision is to join or not join a certain platform. Once they decide to join, they are expected to fiercely compete with other sellers of similar products and will not be significantly affected by marginal changes on the other side of the platform (i.e., customers). Only in the event of a significant decline in the number of customers may the seller revisit its decision to participate in the marketplace, deciding to exit the platform. Therefore, in online marketplaces, there will usually be many different relevant product markets, with different sellers

competing against each other. The definition of these one-sided relevant markets will usually follow the traditional methodology, focusing on demand and supply substitution.[154] Another issue here may be whether these sellers also compete with bricks-and-mortar sellers of the same products, which is an empirical question that may have different answers according to the product under analysis and where the transaction is taking place (depending on differences in convenience, availability, pricing, and consumer habits, which may change over time and across different regions/countries).

In addition, some owners may also join a given side of the platform—becoming sellers like Amazon Basics or Apple Music. In these cases, we should consider them "hybrid marketplaces," where the owner functions simultaneously as a two-sided platform and as a one-sided seller. When acting directly as a seller, the platform is less subject to the competitive constraints imposed by indirect network effects: the platform owner wants to maximize sales and not necessarily to bring other sellers onboard to fulfill the needs of the consumers. In this sense, whenever a platform owner directly offers products to consumers in its own marketplace, it is acting on the one-sided relevant market of the sale of that particular product, much like any other retailer, and should be treated as such. Again, complex platforms may incorporate, at the same time, both one-sided and multi-sided markets, as well-exemplified by the results of the Apple e-Books investigation discussed above. A potential exception would be when consumers were clearly underserved on that specific product and the owner decides to step in as a seller in order to build or maintain the

[154] For example, in *United States v. Topkins*, the first prosecution for price fixing using an algorithm in e-commerce, the focus was the relevant market of sales of posters within the Amazon marketplace. Information at 2–3, United States v. Topkins, No. 3:15-cr-00201-WHO (N.D. Cal. Apr. 6, 2015).

critical mass of customers necessary to bring value to the whole platform—a narrow case in which the platform owner may still be focused on inter-platform competition.[155]

In the case of hybrid marketplaces, there is a vertical dimension that deserves attention. Indeed, the two-sided relevant market involving platform competition is vertically related to the different one-sided relevant markets of sales of goods, and the platform owner may have conflicting interests as manager of the platform and as a seller.[156] This may lead to various forms of leveraging from one market to the other, limiting competition on the merits regarding the sale of specific products.[157] Any actual infringement will depend on the relevance of the particular marketplace for other sellers and the specific conduct under analysis.

Finally, one also has to acknowledge that even in the case of two-sided markets, platform competition involving online retail marketplaces may also include other partial substitutes that are somewhat more distant than pure marketplaces (step four, define the "boundaries of the market").[158] For example, in the Brazilian Google Shopping investigation, CADE's General-Superintendence opinion defending the dismissal of the case (later confirmed by the majority of CADE's Tribunal) recognized that the Google Product Listing Ads (PLAs) tried to convert ads

---

[155] Nonetheless, even in this case one has to consider that the platform may use some less-impacting alternative strategies of intra-platform balancing to promote the underserved product, such as subsidizing parties on that side (think of credit cards awarding miles). This would reinforce the view that even in those cases a single-sided market is probably the better decision.

[156] This vertical issue is in the core of the EU investigation regarding Amazon. *See* Rochelle Toplensky & Shannon Bond, *EU Opens Probe into Amazon Use of Data About Merchants*, FIN. TIMES (Sept. 19, 2018).

[157] This is the essence of the complaints not only against Amazon, but also the Spotify complaint against Apple. *See* Philip Blenkinsop, *Spotify Files EU Antitrust Complaint Against Apple*, REUTERS (Mar. 13, 2019). It is beyond the scope of this article to perform a specific market definition for such cases, but understanding the different competition spaces, the intensity of network effects, and the existence of one-sided markets within two-sided platforms is certainly important in assessing these complaints.

[158] For example, to what extent Skyscanner or Google Flights compete with Expedia, Edreams or other websites where one concludes the transaction on the platform.

directly into sales.[159] Thus, the last generation of Google Shopping tools was considered a partial substitute for marketplaces to the extent that the advertising platform is helping to match retailers and consumers, streamlining direct sales. In fact, some advertising platforms and price comparison sites are progressively coming closer to transaction platforms and competing with marketplaces. In contrast, bricks-and-mortar retail stores that were once considered a close substitute to some online marketplaces[160] are moving further apart in consumers' preferences (considering consumer habits, convenience, etc.). These trends increase the difficulties of defining the boundaries of these relevant markets but should not impact the definition of whether these platforms act as multi-sided or one-sided markets.

b. Hotel Bookings and Property Sharing Platforms

A similar rationale applies to hotel bookings (e.g., Booking.com, Expedia, Decolar) and property sharing platforms (e.g., Airbnb, Homely, HomeAway), which function very much like pure marketplaces. These platforms need to bring together hotels, property owners and customers. They strive to create a critical mass on both sides of the platform, which is significantly affected by network effects. Thus, it is reasonable to look at the platform level competition as a two-sided market. One additional question, which is highly dependent on local contexts, is to define boundaries on the extent to which these platforms compete with other forms of accommodation (e.g., offline hotel offers, bed and breakfasts, or traditional short-term leases). Finally, within these

[159] The General Superintendence of CADE considered Google Shopping and marketplaces like Amazon as differentiated products that exerted some competitive pressure on each other, but this was insufficient to include both in the same relevant market. For a brief description of the SG opinion, see Janith Aranze, *Google Did Not Harm Consumers, CADE Investigators Say*, GLOBAL COMPETITION REV. (Nov. 21, 2018).

[160] For an early discussion of the substitution between digital marketplaces and bricks-and-mortar retailers, see Jared Kagan, Note, *Bricks, Mortar, and Google: Defining the Relevant Antitrust Market for Internet-Based Companies*, 55 N.Y. L. SCH. L. REV. 271 (2011).

platforms, suppliers (i.e., property holders, hotels, and other accommodation providers) compete for customers in typical one-sided markets.

As other intermediaries join these platforms, they create broader ecosystems where new competition spaces and vertical relationships appear. For example, the past few years have witnessed the emergence of firms offering services to owners who list their property in these sharing platforms but do not want to manage the listing or the property itself.[161] These firms compete for property owners, offering "hosting services" for a fee. In doing so, they also aggregate supply in the platform, managing several properties in the same location. They also establish vertical relationships with the property owners and the platform itself. The competition among these intermediaries is one-sided as they simply charge fees for service provided to property owners. However, they may also affect competition at the platform level, as they tend to increase multi-homing, listing the properties they manage in several platforms in order to expand the likelihood of finding a guest. This may increase inter-platform competition and, as these service providers grow, they may even become multi-sided platforms themselves.

Understanding these different competition spaces and their dynamic relationship within and across platforms provides a more accurate analysis than simply considering property sharing platforms as a single two-sided relevant market.

c. Transport Network Companies (TNCs/Ride-sharing Apps)

Ride-sharing apps (e.g., Uber, Lyft, Cabify) are another good example of transaction platforms: they bring together riders and drivers, with observable transactions (rides), charging per

[161] Hostmaker, Bnbsitter, and Houst (formerly Airsorted) are good examples of fast-growing intermediaries that render services to property owners and in doing so may aggregate supply. *See Why Hostmaker?*, HOSTMAKER, hostmaker.com/gb/airbnb-management-services/my-property-portfolio/; *Do Not Remain Seated, Switch to the Mobility Lease*, BNBSITTER, en.bnbsitter.com/; *About Us*, HOUST, www.airsorted.uk/.

transaction fees. In contrast to pure marketplaces or property sharing platforms, where suppliers define their own prices, TNCs tend to establish the price for rides in any given moment. Because of constant large fluctuations in supply and demand (due to work habits, rush hours, special events, weather conditions, etc.) algorithms constantly adjust prices to clear the market. Drivers and riders then decide whether to use the platform or not, according to the price set and their willingness to pay.

This market design tends to increase the feedback loop between the two sides of the market, as the platform owners must always strive to balance the number of drivers offering rides and the number of riders willing to pay for them. As compared to the independent suppliers in a marketplace, drivers cannot change the price established by the platform algorithm, they can only opt to use or not use the platform at any given moment. The value of the platform depends on the density of supply and demand on both sides across time, and on the equilibrium achieved by the algorithm. In these cases, defining a single two-sided market at platform level tends to be the most appropriate approach. The recognition of the two-sidedness of the market is one of the reasons why antitrust authorities around the world have not found antitrust infringements in the associated pricing algorithms.[162]

Inter-platform competition in this context is quite important. Drivers and users can multi-home and connect to different platforms, increasing cross-platform competition and rewarding the player that better manages supply and demand through the pricing algorithm (among

[162] Brazil and India have recently dismissed cases along these lines. *See* Alexandre Cordeiro Macedo, *Uber: Collusion, or Unilateral Conduct?*, MLEX: AB EXTRA (Dec. 19, 2018), www.iiede.com.br/index.php/2018/12/30/alexandre-cordeiro-macedo-uber-collusion-or-unilateral-conduct/ (in Portuguese); *India's Competition Commission Rejects Price-Fixing Allegations Against Uber and Ola*, REUTERS (Nov. 7, 2018), www.reuters.com/article/us-uber-ola-antitrust-idUSKCN1NC1BE. One of the authors, Pereira Neto, counseled Uber in the Brazilian case.

other services provided). Nevertheless, there is also some intra-platform competition among drivers in terms of supply and quality. Drivers and users are mostly price takers, but their behavior impacts platform balancing in different manners. Drivers cannot take action to balance the platform. Yet, for them, the fewer drivers using the system at a given time, the higher the probability of getting a ride and also the higher the price (given the existence of surge pricing). In addition, some platforms match higher rated drivers with more users, encouraging drivers to provide better services (at least in comparison to their peers). The existence of intra-platform competition allows for some types of behavior to impact a single-sided market. For example, if drivers agree to disconnect simultaneously to trigger a false surge in a given region, this practice could be considered collusion on that side of the market, as drivers are not trying to balance out different sides but simply competing against other drivers for rides.

As with property sharing and marketplace platforms, a complex question is to establish the boundaries of the relevant market regarding other mobility alternatives (taxis, private car hiring, car-pooling, buses, and other means of transportation). This is highly dependent on the local factual context and the ever more complex web of relations among different means of transportation in urban areas.

In sum, better understanding these different competition spaces around online transaction platforms as well as the intensity of network effects in each of these spaces will always be a complex, fact-intensive exercise. Authorities and courts must acknowledge and evaluate the possible co-existence of two-sided and one-sided markets in these platforms in order to perform a more accurate analysis.

VII. TOWARDS A MULTI-LAYERED APPROACH TO RELEVANT MARKET DEFINITION IN TRANSACTION PLATFORMS AND THE AGENDA AHEAD

This article has argued that the Supreme Court decision in *Amex* incorporated some of the important advancements in the scholarly understanding of two-sided markets but established a more rigid framework to market definition than the literature warrants. The majority's opinion asserts that two-sided transaction platforms will generally constitute a "single relevant market" for purposes of antitrust analysis, ignoring that platforms may also present other sub-dimensions of competition that may be equally or more relevant for the analysis. In contrast, the minority's opinion sticks to the tradition of narrow definition of relevant markets, ignoring the special competitive dynamic created by indirect network effects (which is distant from Justice Breyer's example of tires and gasoline as complementary goods).

These definitions of relevant markets in two-sided transaction platforms do not fully incorporate the findings of a long-established literature on industrial organization, as well as the rich experience in international cases: different firms engaged in multi-sided markets may have, and respond to, different economic incentives.

The "layered competition approach" proposed in this article is an important way to conceptualize how this dynamic operates by allowing regulators and courts to recognize different levels of interaction: at ecosystem level including several applications (e.g., iOS v. Android), at platform level including multiple players participating in the platform (e.g., Visa v. Mastercard v. American Express), or even at different sides of the platform (e.g., only suppliers in marketplaces; only issuers or acquirers in payment cards; only drivers in ride-sharing apps). Depending on the issue under evaluation, authorities and courts should focus on one or more of these layers as their

primary relevant markets, but they should not ignore that this competitive space is inserted in a more complex platform environment.

In this context, as in many others, any sound definition of relevant market must focus on identifying the competitive constraints of the firms under analysis. It is essential to acknowledge that multiple layers of competition within and across platforms may have different exposure to indirect network effects. Network effects strong enough to effectively limit competitive strategies justify the definition of a single two-sided relevant market. However, even transaction platforms may host competition spaces where firms are relatively insulated from these externalities. The unconstrained behavior of agents in these spaces requires the definition of a one-sided relevant market within the platform. The assessment of the electronic payments industry in the European Union and Brazil, although still lacking a systematic approach, illustrates how these different dimensions of competition are at play in different cases.

Based on these insights and examples, this article proposes a policy-oriented framework structured in a four-step approach that helps authorities separate one-sided and two-sided relevant markets in transaction platforms. Initially, the authority must understand the structure of the platform and the existing competition spaces. Then, it must focus on the side of the market affected by the conduct or merger under evaluation to define a provisional one-sided relevant market. Then, the analysis should consider network effects and their intensity, before expanding the definition to a two-sided market. In order to do so, and considering the difficulties of applying quantitative tests to assess the intensity of network effects, we presented a list of indirect evidence that can be used as part of a qualitative analysis. Finally, the authority has to set the boundaries of this market, considering the substitutability of products. This framework also acknowledges the possible coexistence of different relevant markets within and across transaction platforms, seeking to

explain the potential interaction among different competitive layers. Such a multi-layered perspective is superior to alternative proposals that rigidly require either the definition of a single two-sided market or the definition of multiple one-sided markets.

This conclusion holds beyond the market for electronic payment cards, opening space for a more general application of a multi-layered approach to relevant market definition in transaction platforms. Some platforms may stimulate competition in one side of the market. Others use algorithms to establish the market-clearing price while allowing for competition among sellers over quality, or opt for vertical integration into one side of the platform, limiting intra-platform competition and enhancing inter-platform competition. Understanding the structure of different platforms, how they enable different competition spaces, as well as the interaction among them, is crucial for competition law enforcement.

This multilayered approach is also aligned with the theoretical underpinnings for why antitrust scholars and authorities should think seriously about diminishing the importance of strict boundaries of relevant markets vis-à-vis the actual evaluation of the impacts of a given conduct over an industry (or sub-segments of that industry) when dealing with multi-sided platforms.[163] Indeed, understanding the existence of multiple layers of competition in these platforms will make it easier to assess how a particular conduct or merger impacts one or more of these layers. The antitrust analysis becomes less of a dispute on which analytical lenses should be used, as in the *Amex* decision, and more of a dispute about the understanding of the different incentives, competitive constraints, economic dynamics, and potential harms at stake. Paradoxically, a more

[163] *See* OECD, *supra* note 1; Filippo Maria Lancieri, *Digital Protectionism? Antitrust, Data Protection, and the EU/US Transatlantic Rift*, 7 J. ANTITRUST ENFORCEMENT 27 (2019).

nuanced approach to relevant markets in transaction platforms will increase predictability and give authorities and courts a harder edge to deal with competitive issues in these industries.

This is a potentially fruitful stream of research. It could transcend the opposition between excessively broad or excessively narrow relevant market definitions. In doing so, it will help increase legal certainty for private parties, regulators, and courts, no small feat.

Essay 3:
Narrowing Data Protection's Enforcement Gap

INTRODUCTION

The 2016 European General Data Protection Regulation (GDPR)[1] was hailed as ushering a new era for digital privacy. It led companies and European countries to invest significant resources in designing regulatory compliance programs.[2] It also influenced many other online privacy laws adopted across the world—including, to some extent, the groundbreaking California Consumer Privacy Act of 2018 (CCPA).[3] Yet, years afterwards privacy advocates are growing increasingly frustrated with firms lack of compliance and countries lax enforcement. Indeed, the gap between the law on the books and the law in action appeared to be so great that by the end of 2020 many of the GDPR's strongest supporters warned that it risked becoming a "fantasy law", something

---

* This Article is forthcoming in Maine Law Review Volume 74, Issue 1 (2022). It is reprinted here in accordance with the Maine Law Review Copyright Policy.

[1] General Data Protection Regulation 2016/679, 2016 O.J. (L 119) (EU).
This paper uses interchangeably data privacy, online privacy, data protection and digital privacy to refer to limits on the collection and processing of personal data.

[2] PriceWaterhouseCoopers, *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*, PWC (2017), http://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.

[3] See Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N. Y. UNIV. LAW REV. (2019) at 107; Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. (2021), at 1764. By 2020, 142 countries passed some form of data protection legislation, 62 in the past 10 years. Graham Greenleaf & Cottier Bertil, *2020 ends a decade of 62 new data privacy laws*, 163 PRIV. LAWS BUS. INT. REP. 24 (2020).

firms paid lip service to but nonetheless widely failed to comply with.[4] Frustration with the CCPA was equally widespread, leading privacy advocates to immediately start drafting a new law to strengthen its enforcement mechanisms—the California Privacy Rights Act (CPRA) passed the ballot vote in November 2020 and will come into force in 2023.[5]

Concerns around an enforcement gap in data protection laws are sensible: older digital privacy regimes in Europe and the United States have largely failed to ensure that companies' comply with consumers' preferences for increased control over their personal data.[6] While it is too early to decree the failure of newer regimes such as the GDPR and the CCPA, most of the available analyses also point to underwhelming results: since the entering into force of both laws, none of twenty-two independent empirical studies conducted to assess their impact on the ground found meaningful legal compliance. For example, a 2019 academic survey found that 92% of Europe's most accessed websites tracked users before providing any notice and 85% maintained or increased tracking even after the users opted-out, both clear violations of the GDPR;[7] a cookie sweep of 38 large data processors performed by the Irish Data protection authority found that more than 18 months after the GDPR had come into force, 92% did not comply with the law;[8] another report

[4] Adam SATARIANO, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, THE NEW YORK TIMES, April 27, 2020, https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html.
[5] See California Proposition 24: The California Privacy Rights Act of 2020, available at https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.
[6] See Part I.B and Annex I below.
[7] Iskander Sanchez-Rola et al., *Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control*, *in* PROCEEDINGS OF THE 2019 ACM ASIA CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 340–351 (2019) at 341; 344-345, (analyzing 2.000 high profile EU websites).
[8] See Irish Data Protection Commission, *Report by the Data Protection Commission on the use of cookies and other tracking technologies* (2020), https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Report%20by%20the%20DPC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf, at 6.

exposed how European data authorities are underfunded and poorly staffed.[9] There are fewer comprehensive analyses for the CCPA (it only came into force in January 2020), but the law apparently led to no changes to Facebook's data collection and processing practices,[10] a survey of the US' 600 largest companies' websites conducted in February 2020 found that even among the richest, most sophisticated American companies, a majority of did not offer CCPA portals for users to access their information—in some important sectors such as Technology, Media and Telecom and Health Services, only 40% of companies did so[11]—and another survey of Business-to-Consumer companies found that these businesses are receiving on average 11 data-related requests per month for every million California consumer identities they hold, meaning that the CCPA was being used by 0.001% of Californian consumers.[12] The very passage of the CPRA represented an admission that, despite its broad promises, the CCPA is unlikely to meaningfully improve consumer data privacy.

These findings raise two questions for academics and policymakers (i) are there important gaps in the enforcement mechanisms of data protection laws? and, if yes, (ii) what can be done to improve their performance?

This paper helps answer both puzzles. First, it suggests that modern data protection laws largely fail to anticipate how exceptionally large information asymmetries and market power present in

[9] BRAVE, *Europe's governments are failing the GDPR* (2020), https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf, at 3, 6.
[10] Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL STREET JOURNAL, December 12, 2019, https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345.
[11] See PriceWaterhouseCoopers, *CCPA in Financial Services: Early Operational Benchmarks* (2020), https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/california-consumer-privacy-act/ccpa-financial-services.html
[12] Data Grail, *The State of CCPA: Benchmarking CCPA Trends Across Consumer (B2C) Brands* (2021), https://www.datagrail.io/the-state-of-ccpa/. at 4.

many data markets undercut legal compliance in the shadows of the law. Second, it examines the institutional design of antitrust and anti-corporate fraud laws—both established legal regimes that face similar challenges with regards to information asymmetries and market power undermining compliance—to propose legal and institutional changes that can help narrow this enforcement gap in data protection.

In order to do so, this paper is divided in three parts. Part I briefly outlines the rise of data protection laws in the US and the EU, and reviews the empirical literature on their (so far limited) impact on the ground.

Part II, the core of the paper, explores how Americans and Europeans designed their legal regimes to harness (different) combinations of market forces, tort liability and regulatory enforcement as mechanisms to ensure that companies reflect consumers' privacy preferences. Yet, if consumers cannot understand price/quality ratios in products that produce or rely on personal data, they cannot take advantage of the traditional options of exit (switching suppliers) and voice (complaining to management) as strategies to force companies to comply with their preferences. Similarly, if consumers and lawyers cannot identify problems in products/services or link them to recognizable legal harm, they cannot rely on tort lawsuits as an alternative to punish non-compliant companies. Finally, the opacity and complexity of data markets undermines regulatory enforcement in two distinct manners: (i) it increases the opportunities for companies to distort regulations to their advantage without facing significant political backlash; and (ii) it expands the public resources needed to maintain a regulatory regime dedicated to discover and successfully prosecute violations. Lawmakers also failed to anticipate how market power allows some companies that collect and process a significant amount of personal data to behave strategically to protect private interests and undermine legal compliance in the shadows of the law. In particular, dominant digital

platforms rely on the economic and political capabilities associated with their market power to: (i) design data markets in ways that exacerbate their inherent information asymmetries; (ii) further undermine consumer exit and voice strategies; (iii) combat tort litigation and regulatory enforcement; and (iv) influence governmental policy to their advantage.

While these are relevant flaws in the design of data protection laws, they are not unsurmountable. Part III explores how policymakers can learn from the experience with the enforcement of antitrust and anti-corporate fraud laws to design changes that can help narrow this enforcement gap. Focusing on the institutional alternatives to diminish information asymmetries in the enforcement of data protection laws,[13] the paper suggests that online privacy regulatory systems should be built around at least three key principles.

First, the system must multiply monitoring and enforcement resources. In particular, sophisticated civil-society intermediaries such as privacy NGOs, independent think-tanks, investigative journalism outlets and class-action plaintiffs play an outsized role in ensuring deterrence and protecting consumers in opaque and complex markets. That is because these organizations have the incentives and the capacity to develop the skills to understand the complexity of data collection and denounce violations. In doing so, they can also monitor the performance of regulatory agencies and increase the costs of regulatory capture. A comparative look at antitrust policy provides a valuable example of how data protection laws can use the resources raised by public fines, grants and *cy pres* awards to properly fund these sophisticated intermediaries, ensuring that they have the

[13] Antitrust scholars are increasingly focused on tackling the market power of digital platforms. See Filippo Lancieri & Patricia Sakowski, *Competition in digital markets: A review of expert reports*, 26 STANF. J. LAW BUS. FINANCE (2021) for a review of expert reports proposing antitrust and regulatory interventions to diminish the market power of companies such as Google, Facebook, Apple and Amazon.

necessary means to perform their institutional role while ensuring their independence from industry interests (and deep pockets).

Second, the combination of broad scope, opacity and complexity that characterizes data protection encumbers the detection of legal violations, increasing the resources needed for society to identify non-compliance. To countervail that, the enforcement system should be designed to bring violations to the attention of monitors. Antitrust and anti-corporate fraud policies have long relied on leniency and whistleblower programs as a way to encourage insiders to reveal wrongdoing. Data protection laws should learn from their example and develop a solid whistleblower program to help bring violations to light.

Third, public enforcement systems must ensure that regulators are accountable to civil society. Data is a key input to national security and to companies competing in a digital world—so governments have legitimate interests to enable the widespread collection of personal data. A combination of governmental interests, the market power of large digital platforms and the complexity/opacity that characterizes many data markets increases the risks that regulators promote industry rather than consumers' interests. An aggravating factor is that modern data protection regimes lack institutional safeguards that can help thwart regulatory capture—while transparency is key to help societies fight powerful, vested interests, many data protection agencies are absolutely opaque. Antitrust regimes can provide an example on how to design a regulatory framework that increases transparency without sacrificing enforcement capacity.

A brief conclusion follows.

I. THE RISE OF DATA PROTECTION LAWS

i. Data protection on the books

Privacy rights were first developed in the United States and in Europe to safeguard individual dignity, autonomy and preserve some form of information self-determination.[14] A right to privacy naturally includes the protection of personal information that citizens do not want disclosed[15] and the increasingly important role databases containing personal data started playing in citizens' lives during the second half of the 20th century motivated the expansion of this "right to informational privacy" to incorporate some form of "right to data protection".[16]

The EU was among the first jurisdictions to enact, in 1995, an economy-wide Directive specifically focused on imposing limits on the collection and processing of personal data.[17] Widespread concerns around its lack of effectiveness, however, motivated the passage of the GDPR in 2016.[18]

---

[14] For a summary, see Filippo Lancieri, *Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift*, 7 J. ANTITRUST ENFORC. 27–53 (2019), at 30.

[15] Lior Strahilevitz, *Reunifying Privacy Law*, CALIF. LAW REV. 2007–2048 (2010), at 2016.

[16] Fred H. Cate, *The failure of fair information privacy principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343–379 (2006), at 345. Riley v. California, 134 Ct 2473, 2489 (2014) (concluding that modern day smartphones hold so much personal data that law enforcement needs a warrant to search them). The US led this recognition of a right to data protection by passing the 1970 American Fair Credit Reporting Act and the 1974 Privacy Act, as well as a series of statutes that oversee the collection of specific data such as health or children. At the EU level, this transition started with a 1981 convention, a 1995 Directive and then Article 8 of the EU Charter on Fundamental Rights, which affirms data protection as a fundamental right.

[17] Directive 95/46/EC required EU member states to impose limits on the basis under which companies can collect and process personal data, created rights of access and rights of rectification and required the creation of dedicated regulators (among others). It is complemented by Directive 2002/58/EC (the "ePrivacy Directive") which requires that users are properly informed and consent to being tracked by certain types of cookies and other online tracking methods, among other protections for electronic communications.

[18] Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. LAW REV. 1966 (2013), at 1969-1971.

The GDPR grants EU citizens strong rights with regards to their data and also imposes a series of obligations on governments and companies that handle such data.[19] Noteworthy provisions include requirements that data are processed in lawful, fair and transparent manner, that users grant "explicit consent" to enable the collection and processing of data;[20] data minimization and purpose limitation; a right to be forgotten and to data portability; data protection by design and by default; minimum requirements around data security; an obligation that companies perform impact assessments for new technologies or new uses of data and notify users about data breaches; the strengthening of data protection authorities; and a right for citizens to go to Court to directly obtain full compensation for damages associated with violations of data protection laws.[21]

The US lacks a similar economy-wide data protection regime, historically relying on the Federal Trade Commission (FTC) as a de-facto online privacy regulator.[22] The FTC enforces a regime of *informed consent,* where it mostly ensures that companies disclose to consumers how they collect and process data so that consumers can make an informed decision on whether to accept these terms in a take-it-or-leave-it fashion.[23] The FTC does not impose general limits on how personal data is collected or processed. Except in specific contexts, the agency lacks power to impose fines or other non-voluntary punishments, and the Supreme Court recently greatly curtailed its power to

[19] For a summary, see Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union general data protection regulation: what it is and what it means*, 28 INF. COMMUN. TECHNOL. LAW 65–98 (2019).
[20] GDPR art. 7. Consent is one out of six legitimate reasons for the collection and processing of personal data (see art. 6)
[21] GDPR arts. 5, 16, 17, 20, 25, 32-35, 51, 52, 57, 58, 77-83. EU Data Protection authorities can fine companies up to 4% of their worldwide turnover for violations.
[22] Lancieri, *supra* note 14, at 32.
[23] Daniel Solove & Woodrow Hartzog, *The FTC and the new common law of privacy*, COLUMBIA LAW REV. 583–676 (2014), at 592.

mandate the disgorgement of illegal profits.[24] Enforcement is ex-post and focused on fraud or clear misstatements.

The lack of a Federal law combined with the fact that most large tech platforms are based in California means that the CCPA, passed in 2018, is the leading US consumer data privacy regulation.[25] The CCPA is both narrower in scope than the GDPR and reflects fundamental differences in the role privacy plays in society.[26] Nonetheless, it represents a significant expansion over the simple informed consent doctrine. Noteworthy provisions include: stronger notification requirements for the collection and processing of personal data; a right of access and of erasure; a right to object against the selling of personal information; an obligation that companies create "data portals"; a right to data portability; and a direct right of action for damages in cases of data breaches (up to USD 750 per incident or actual damages, whichever is greater). The Office of the California Attorney General holds exclusive powers to enforce most CCPA provisions (with the exception of data breaches) and is also responsible for updating the terms of the regulation.[27]

In 2020, Californians passed the CPRA through a direct ballot, amending and expanding the CCPA to strengthen its enforcement mechanisms. The CPRA's main additions are creation of a subgroup of sensitive personal data, expanded disclosure requirements, the expansion of the consumers' right to know to include all personal data that businesses sell *or share* for purposes of digital advertisement, including the right to opt-out of both processes through a "do not sell or share" and

[24] *Id.* at 604-605 and AMG CAPITAL MANAGEMENT, LLC v. Federal Trade Commission, 593 U.S. (2021).
[25] Chander, Kaminski, and McGeveran, *supra* note 3, at 1769.
[26] Lancieri, *supra* note 14, at 31 (explaining how Europeans treat data as a fundamental right, while Americans treat data as an asset).
[27] CCPA Secs. 1798.100, 1798.105, 1798.110, 1798.125, 1798.130, 1798.150, 1798.155 and 1798.185. Penalties vary between USD 2500 per normal violation and USD 7500 per intentional violation.

a "limit the use of my sensitive personal information" button; a right to limit the use and disclosure of sensitive personal data; the creation of the California Privacy Protection Agency—a regulatory agency with powers to enact regulations and impose administrative fines—and the determination that 9% of a fund that collects data protection fines should be annually distributed to civil society as grants.[28]

The GDPR and the CCPA, even after amended, are distinct bodies of law that differ in many important manners.[29] Yet, at their core they reflect a general belief that companies were not responsive to (at least some) citizens' preferences for increased control over how their personal data is collected and processed.[30]

The GDPR, for example, was passed partially in response to widespread concerns by European citizens regarding the collection and processing of personal data—67% of Europeans were concerned about not having complete control over their personal data, 70% were concerned about mismatches between information collection and processing and 90% believed it was important to have similar data protection rights across the EU.[31] The Regulation states that a central tenet of data protection is that Europeans know what type of personal data is being collected about them,

[28] CPRA, Secs. 8, 9, 10, 12, 13, 14, 17, 18 and 24. The California privacy protection agency can impose administrative fines of up to USD 2500 per each non-intentional violation of the law and USD 7500 per each intentional violation (CCPA Sec. 1798.155, as amended by the CPRA Sec. 17).

[29] See Chander, Kaminski, and McGeveran, *supra* note 3, at 1746 (comparing the GDPR and the CCPA and concluding that they offer "a fundamentally different regime for data privacy").

[30] GDPR recitals 7 and 11 expressively states that "Natural persons should have control of their own personal data" and that this requires the development of a strong regime to ensure compliance. The CPRA Section (2)(h) states that "People desire privacy and more control over their information. California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information."

[31] GDPR recitals 7, 9 and 11; European Commission, *Special Eurobarometer 431 - Data Protection* (2015), at 6-7.

and how it is processed.[32] It is also expressively designed to address short-comings with the enforcement of older European data protection regimes by creating a system that protects these fundamental privacy rights and ensures compliance.[33]

Somewhat similarly, a majority of Americans is concerned about data harvesting by corporations—81% of respondents to a 2019 survey indicate that they lack control over their personal data and that the risks of data collection outweigh the benefits, 79% are concerned that data is being misused.[34] By passing the CCPA, California's legislature explicitly intended to give California consumers "an effective way to control their personal information" by giving them the right to: (i) "to know what personal information is being collected about them"; (ii) "to know whether their personal information is sold or disclosed and to whom"; (iii) "to say no to the sale of personal information" and (iv) "to receive equal service and price, even if they exercise their privacy rights".[35] The CCPA was initially slated to be subject to a public vote and the wide expectation over its passage forced the industry to cut a legislative deal.[36] The CPRA—proposed to strengthen these enforcement mechanisms—won the public vote by a landslide and expressively states that consumers are not aware of how companies collect and process personal data, that they

[32] GDPR Recital 39. Chander, Kaminski, and McGeveran, *supra* note 3, at 1750.
[33] GDPR recitals 9 and 11.
[34] See Pew Research Center, *Americans and privacy: Concerned, confused and feeling lack of control over their personal information* (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf, at 4; and also Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The economics of privacy*, 54 J. ECON. LIT. 442–92 (2016), at 476 (stressing how survey and other evidence indicates that the protection of personal privacy is a leading concern in the US).
[35] CCPA Sec. 2(i).
[36] CPRA, Sec. 2(c) and Chander, Kaminski, and McGeveran, supra note 3, at 1781-82 (describing the disputes surrounding the passage of the CCPA).

need stronger laws to protect their fundamental privacy rights, and that the Government of California must strengthen the enforcement of these rights over time.[37]

Some discount this clear preference for increased data control, asserting that while citizens submit they want increased protection, they trade their personal data for small incentives—an apparent contradiction known as the *privacy paradox*.[38] Yet, the existence of a strong "paradox" has been largely dismissed by more recent literature. While some disconnect between stated privacy preferences and actual personal behavior exists there is "ample and enduring" evidence that consumers recurrently act to protect their privacy in both online and offline scenarios.[39] Indeed, most paradoxical cases can be explained by the fact that data protection is "extraordinarily difficult to manage, or regulate, in the internet age" as firms explore known limitations in consumer rationality to extract as much personal information as viable.[40]

That is not to say that every citizen has strong preferences for increased data protection, nor that these laws are perfect—the GDPR and the CCPA have been praised by many,[41] but criticized by some who believe they harm innovation, replace consumers' preferences by regulators' preferences and stifle free expression.[42] Rather, they reinforce that consumers' persistent call for

[37] CPRA, Sections 2(e)(f)(g) and (h).
[38] Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, J. CONSUM. PSYCHOL. (2020), at 737; 749.
[39] *Id.*, at 737. Acquisti, Taylor, and Wagman, *supra* note 34, at 477-478. These range from simple analysis of consumer behavior to surveys, field studies, experiments and other pieces of data.
[40] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 740-744; 750. Numerous processes negatively impact privacy-related rational decision-making in specific circumstances, from extreme information asymmetries to bounded rationality, hyperbolic discounting, resignation, herding or cognitive and behavioral biases.
[41] Schwartz, *supra* note 3, at 102.
[42] see Roselin Layton, *The 10 Problems of the GDPR - Statement before the Senate Judiciary Committee* (2019), https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf

better data protection should be accounted for.[43] A key reason behind democratically elected governments in California and the EU passing the largely popular CCPA, CPRA and GDPR is exactly because they found a disconnect between citizens preferences for increased protection and control of their personal data, and market practices ignoring these preferences. Equally important, these laws are leading to billions of dollars of investments in compliance programs.[44] Societies must ensure that these expenditures actually change market practices.

ii. An underwhelming track-record (so far)

Yet, despite these bold ambition, the historical track-record of data protection laws in the EU and the US is underwhelming. A solid body of work shows how private parties never complied with the commands of two European data protection directives that preceded the GDPR.[45] By one account, almost 75% of EU websites constantly violated the rules without suffering any form of punishment.[46] Across the Atlantic, even governmental authorities have deemed the FTC's lack of powers to fine firms for data-related violations as incapable of ensuring meaningful regulatory deterrence, and this was before the Supreme Court largely gutted its capacity to disgorge illegal profits, leaving the agency almost powerless.[47] A general diagnosis is that the Fair Information

[43] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 750.
[44] See PriceWaterhouseCoopers, *supra* note 2; Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH UL REV 773 (2019), at 777, 803-07 (describing the large "paper trails" created by privacy compliance programs, but that do not materially improve data protection).
[45] See Ronald Leenes & Eleni Kosta, *Taming the cookie monster with dutch law–a tale of regulatory failure*, 31 COMPUT. LAW SECUR. REV. 317–335 (2015), at 329.
[46] Martino Trevisan et al., *4 years of EU cookie law: Results and lessons learned*, 2019 PROC. PRIV. ENHANCING TECHNOL. 126–145 (2019), at 127, 133, 140 (surveying 35.000 popular EU websites and finding that 49-74% placed tracking cookies before receiving consent, a violation of the directive).
[47] A wide review of FTC enforcement actions by the Government Accountability Office concluded that all but a handful of FTC cases ended up in settlements and recommended the development of a strong regulator with the capacity to regulate the market and impose broad civil penalties. United States Government Accountability Office, *Internet Privacy: Report to the*

Privacy Principles (the foundation of legacy data protection regimes in both sides of the Atlantic) have largely failed to achieve their stated goals of aligning consumers' and companies' privacy preferences and increasing data protection.[48] Private self-regulation has not fared any better.[49] That is mainly because these older laws were "*toothless"* or *"paper tigers*".[50]

The GDPR and the CCPA were partially designed to address these shortcomings.[51] Changes in the GDPR, for example, were specifically aimed at bringing data protection closer to antitrust in terms of enforcement, fining capacity and others.[52] Issuing a definitive judgement on the performance of these laws is complicated for at least two reasons: first because these are new and complex regulatory regimes, so it is perfectly possible that enforcement is suboptimal in the first years but improves as regulations mature; second, because many data protection markets are so opaque that reliable evidence for empirical studies is hard to obtain.

Still, these limitations notwithstanding, Annex I contains a comprehensive survey of studies that have independently assessed compliance with the commands of the GDPR and, to a lesser extent, CCPA. The available evidence consistently indicates an underwhelming impact of these new regimes—out of twenty-two independent evaluations, *none* found that these laws led to meaningful increases in data protection. For example, a survey of privacy protection policies of almost 200

Chairman, Committee on Energy and Commerce, House of Representatives (2019), https://www.gao.gov/assets/700/696437.pdf, at 37. See also AMG CAPITAL MANAGEMENT, LLC v. Federal Trade Commission, 593 U.S. (2021).

[48] Cate, *supra* note 16, at 344.

[49] See, generally, Robert Gellman & Pam Dixon, *Failures of privacy self-regulation in the united States*, *in* ENFORCING PRIVACY 53–77 (2016).

[50] Sebastian J. Golla, *Is data protection law growing teeth: The current lack of sanctions in data protection law and administrative fines under the GDPR*, 8 J INTELL PROP INFO TECH ELEC COM L 70 (2017) at 70, Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 93, (also stressing how "the directive [95/46] was plagued by ineffective sanctions". Both refer to European data protection laws but the conclusion can easily be extended to the FTC).

[51] Schwartz, *supra* note 18, at 1969-1971.

[52] Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 67, 92.

large firms before and after the GDPR found that while the legislation led to textual changes "the overall level of compliance [with GDPR provisions] is not high in absolute terms"; a 2019 review of the EU's 2000 most-accessed websites found that 92% of them tracked users before providing any notice, 85% maintained or increased tracking even after the users opted-out, violating the Regulation;[53] these findings are backed by another study analyzing the 500 most visited websites in each EU country, finding that the amount of user tracking pre and post-GDPR stayed the same—the study warned against a false sense of GDPR compliance.[54] Even EU authorities are finding widespread violations, as shown by a survey of 38 large data processors performed by the Irish Data protection authority that found that more than 18 months after the GDPR had come into force, 92% did not comply with the law.[55] There is less such independent data on CCPA compliance, but the trend is similar. A February 2020 PwC survey of the websites of the US' 600 largest companies reported that even among these large, very sophisticated companies, a majority did not offer portals for users to access their information.[56] An April 2021 report survey of Business-to-Consumer companies found that these businesses are receiving on average 11 data-related requests per month for every million California consumer identities they hold, meaning that the CCPA was being used by 0.001% of Californian consumers.[57] While not specifically targeted at the CCPA, a September 2020 scan of more than 80.000 of the world's most popular websites by US-based investigative journalism website The Markup found that tracking remains ubiquitous around the world and in the US, even in highly sensitive websites such as those of abortion providers or for victims of

[53] Sanchez-Rola et al., *supra* note 7, at 341, 344-345, (analyzing 2.000 high profile EU websites).
[54] Martin Degeling et al., *We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy*, ARXI ARXIV180805096 (2018), at 7-8, 10, 14.
[55] See Irish Data Protection Commission, *supra* note 8, at 6.
[56] PriceWaterhouseCoopers, *supra* note 12.
[57] Data Grail, *supra* note 13. at 4.

sexual violence.[58] Its general conclusions are that third-party tracking is as pervasive now as it was 10 years ago, but it has only "become creepier and more difficult to stop".[59]

These conclusions are backed by other pieces of evidence. After a detailed analysis of companies' internal data protection compliance practices, Professor Ari Waldman described the GDPR and the CCPA as a "house of cards" that is failing to deliver on its promised protections because companies privilege hollow, formal compliance over actual substance.[60] European data protection agencies received more than 275.000 complaints in the first eighteen months since the GDPR came into force, but by then they had issued only 785 fines.[61] Data protection agencies are generally underfunded and poorly staffed: "nearly every European government underfunds its DPA" and regulators in all jurisdictions (but Germany) lack tech specialists.[62] The head of the Irish data protection agency[63] graded her own agency's two-year GDPR enforcement performance as an "A for effort" but a "C-plus/B-minus in terms of output".[64] The head of the German Data Protection authority summarized the situation as: "we have a problem of enforcement";[65] and the head of the Hamburg data protection authority is "completely critical of the enforcement structure

[58] See The Markup, *The High Privacy Cost of a "Free" Website* (2020), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites.
[59] The Markup, *What They Know … Now* (2020), https://themarkup.org/blacklight/2020/09/22/what-they-know-now.
[60] Waldman, *supra* note 44, at 776, 786, 803.
[61] European Commission, *Staff Working Document Accompanying the 2-year GDPR Review* (2020), https://ec.europa.eu/info/sites/info/files/1_en_swd_part1_v6.pdf, at 20;
[62] Brave, *supra* note 9, at 3, 6.
[63] The data protection authority responsible for overseeing Google, Facebook, Apple, Twitter and other large tech platforms.
[64] Satariano, *supra* note 4.
[65] *Id.*

of the GDPR (…) the whole system doesn't work".[66] On the other side of the Atlantic, when asked about the enforcement of the CCPA the California Attorney General stated that the lack of resources would force the agency to look kindly on companies that simply "demonstrate an effort to comply [with the law]".[67] Californians passed the CPRA to fill-in what they identified as clear gaps in the enforcement structures of the CCPA.

As Professor David Erdos aptly summarized "with ever increasing digitization, the gap between the [privacy] law on the books and the implementation and enforcement on the ground [initially described as very large] is almost certainly growing".[68] Given this somewhat discouraging background, academics and policymakers hoping to improve the performance of data protection laws must ask themselves: (i) are there important gaps in the design of data protection laws that enables companies to ignore their commands? and, if yes, (ii) what legal and institutional changes can help improve the performance of these laws?

Parts II and III below help tackle these difficult problems.

II. HOW DESIGN FAILURES UNDERMINE DATA PROTECTION ENFORCEMENT

Online privacy laws such as the GDPR and the CCPA are sophisticated pieces of legislation that rely on different combinations of market forces, tort liability and public regulation to ensure that

---

[66] Vincent Manacour & Mark Scott, *Two years into new EU privacy regime, questions hang over enforcement*, POLITICO, 2020, https://www.politico.eu/article/europe-data-protection-privacy-gdpr-anniversary/.
[67] Nandita Bose, *California AG says privacy law enforcement to be guided by willingness to comply*, REUTERS, 2019, https://www.reuters.com/article/us-usa-privacy-california-idUSKBN1YE2C4.
[68] David Erdos, *Feedback on Report on the Application of the General Data Protection Regulation* (2020), https://inforrm.org/2020/05/05/acontextual-and-ineffective-reviewing-the-gdpr-two-years-on-david-erdos/, at 2.

companies act in accordance with consumers' privacy preferences. Yet, a particularly pervasive combination of large, structural information asymmetries and market power that is present in many data markets undermine all three mechanisms as drivers of legal compliance.

i. Market forces

a. Markets can force companies to reflect consumers' privacy preferences

Markets are the most cost-effective mechanism to ensure that companies reflect consumers' preferences. Yet, information asymmetries and economic power can prevent markets from delivering such outcomes.

More specifically, markets represent the aggregate of two different types of strategic behavior consumers adopt when faced with a decline in the quality of a given good, service or organization: exit or voice.[69] Exit is a binary choice that reflects the invisible hand working at its best—whenever the quality of a good/service goes down, consumers shift to another supplier. Voice is protest—consumers continue buying from the firm but complain to management that the quality is going down. Exit and voice are not mutually exclusive, but exit is the foundation of consumers' ability to discipline companies, as voice requires at least a threat of exit to work. Exit and voice are powerful: *If* markets are competitive and consumers are well-informed, a combination of customers switching and complaining will force companies to supply what consumers desire and ensure allocative efficiency.[70] This aggregation of consumer behavior is a cheap, effective and

[69] 25 ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970), at 4, 21, 30.

[70] Keith Dowding, *Albert O. Hirschman, Exit, Voice and Loyalty: Responses to Decline in Firms, Organizations, and States*, *in* THE OXFORD HANDBOOK OF CLASSICS IN PUBLIC POLICY AND ADMINISTRATION (2015), at 2; Adrian Kuenzler, *Direct Consumer Influence—The Missing Strategy to Integrate Data Privacy Preferences into the Market*, YEARB. EUR. LAW (2020), at 6-8 (providing examples for some segments of the digital economy).

decentralized mechanism that conveys information to firms and enforces heterodox consumer preferences.

Data protection laws have historically endeavored to harness the power of markets as a mechanism to ensure that companies reflect consumer data preferences. As seen above, notice and consent obligations have long been a backbone of data protection laws, even before the passage of modern regimes. Albeit differing in important ways, both the CCPA and the GDPR further strengthened these notice and consent provisions by enabling consumers to access, correct and delete the information companies hold about them and to withdraw consent/stop collection of personal data at any point in time.[71] Both laws also establish (different) minimum levels of information that must be supplied to users before companies can collect their data, including what type and the extent of personal data that is amassed and how it will be processed.[72] Rights to data portability present in both laws—which generally enable consumers to transfer their personal data to alternative suppliers—are another mechanism to release consumers from a potential lock-in due to a company's control over their data. Well-informed, unrestrained consumers can then trigger exit and voice as strategic responses to a bad bargain involving their personal data, forcing companies to account for their preferences.

---

[71] Chander, Kaminski, and McGeveran, *supra* note 3, at 1750 (explaining how both the GDPR and the CCPA contain different provisions to increase transparency over data collection and processing); Wolfgang Kerber & Karsten K. Zolna, *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law* (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3719098., at 18-19 (explaining how the GDPR focuses on addressing information and consumer behavior market failures in data markets, but ignoring concentration aspects, what they call a dual market failure).

[72] For example, the GDPR requires that consent should be specific and unambiguous, that whenever the data processing has multiple purposes a specific consent must be given to each purpose and that clear imbalances between the data subject and the controller may imply that consent was not freely given. Heightened consent requirements apply to specific types of sensitive personal data, such as that about sexual orientation, religion and others. The CCPA just requires general notices.

Markets, however, only work if there is meaningful competition: voice without a credible threat of exit is ineffective, as a monopolist can dismiss consumer discontentment and continue to appropriate rents without much economic loss.[73] Markets also fail when large information asymmetries increase consumers' search costs: the exercise of exit and voice depends on consumers perceiving a decline in quality and acknowledging that alternative suppliers offer better terms. This acquisition of information, however, is costly and many times subject to collective action problems.[74] This is particularly true for complex, opaque goods where it is hard to perceive relative quality.

This failure is also true for many markets where data is a key input, where deep information asymmetries, opacity and economic concentration problems prevent meaningful consumer exit and voice.

b. The heightened information asymmetries in data protection

Information asymmetries abound in data protection and negatively impact consumers' capacity to effectively manage online privacy.[75] Privacy policies run for thousands of words and are usually not designed to optimize consumer understanding[76]—a typical user would spend several weeks a

[73] Dowding, *supra* note 70, at 2-3, 10, 25; HIRSCHMAN, *supra* note 69, at 82, 97.
[74] Dowding, *supra* note 70, at 10.
[75] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 742. Acquisti, Taylor, and Wagman, *supra* note 34, at 448.
[76] For example, an investigation by the British Competition and Markets Authority (CMA) concluded that consumers hardly engage with the privacy controls of Google and Facebook because both companies have strong incentives to maximize consumer data collection, and they actively do so by amplifying information asymmetries and abusing choice architectures in ways that harm consumer choice and consumer privacy. COMPETITION AND MARKETS AUTH., ONLINE PLATFORMS AND DIGITAL ADVERTISING MARKET: FINAL REPORT (2020), https://perma.cc/AJ3F-C44Z, at 149.

year just reading them.[77] As a result, these policies—the main technique to inform consumers about the collection and processing of their personal data—are all but ignored.[78]

Even in a distant, ideal world where companies optimized consumer understanding and consumers read all policies, it would be all but impossible for users to fully comprehend what is done with their data. Data-intensive industries tend to be extremely complex and companies have strong economic incentives to invest in gathering an increasing amount of consumer information.[79] Companies use different and obscure means to collect user data, including sign-in/subscription tracking, cookies, web tags, ad tags, pixels, fingerprinting, mobile apps or cellphone tracking.[80] A traditional user is tracked by an average of at least 20 different companies in its regular web browsing alone,[81] and most mobile apps and devices also collect and share a large amount of personal data.[82] For example, Google collects by default a significant amount of personal data from all Android users, some surveys have found that a median app in the Google Play Store hosts

[77] Alecia M. McDonald & Lorrie Faith Cranor, *The cost of reading privacy policies*, 4 ISJLP 543 (2008), at 563 (estimating that the average American would spend 244h per year (40 min/day) to read all privacy policies it encounters).
[78] The CMA found that that between [0-5%] of Google UK users accessed the company's privacy policies, and 85% of those who did spent less than 10 seconds on the page—probably a misclick. Facebook's had similar numbers of [0-5%] of users accessing its privacy control features over a 28-day period. See Competition and Markets Authority, *supra* note 76, at 173-174.
[79] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 745. Acquisti, Taylor, and Wagman, *supra* note 34, at 463.
[80] For a detailed analysis see AUSTRALIAN COMPETITION AND CONSUMER COMM'N, DIGITAL PLATFORMS INQUIRY - FINAL REPORT (2019), https://perma.cc/3CCL-M3GU, at 130.
[81] Steven Englehardt & Arvind Narayanan, *Online tracking: A 1-million-site measurement and analysis*, *in* PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 1388–1401 (2016), at 10, (surveying 100 random out of the 500 most accessed websites in 16 categories and finding an average of 20 different third-parties tracking users per site).
[82] See Elias P. Papadopoulos et al., *The long-standing privacy debate: Mobile websites vs mobile apps*, *in* PROCEEDINGS OF THE 26TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 153–162 (2017), at 154, 158; Competition and Markets Authority, *supra* note 76, app. G at 37.

trackers by five different companies and 88% of Google Play Apps apparently share back data with Google (43% with Facebook).[83]

Even if users could comprehend the complexity of this data collection network, some forms of surveillance can hardly be prevented by consumers alone: data collection mechanisms such as pixels, web bugs and fingerprinting are effectively invisible to the user;[84] Google does not allow Android users to become fully anonymized to advertisers and all major mobile carriers in the US were fined for selling real-time user location data without consent.[85] Many companies (such as Google and Facebook) responded to data protection laws not by diminishing data collection but rather by embedding their third-party code in first-party applications, something that users cannot block.[86] In theory, "*privacy labels*" or other similar alternatives can help consumers by conveying simple information that users can easily process and incorporate in their decision-making. However, these have failed in other markets in general[87] and in data markets in particular,[88] and

[83] See Reuben Binns et al., *Third party tracking in the mobile ecosystem*, *in* PROCEEDINGS OF THE 10TH ACM CONFERENCE ON WEB SCIENCE 23–31 (2018), at 26; Competition and Markets Authority, *supra* note 76, app. G at 10, app. F at F16.
[84] Acquisti, Taylor, and Wagman, *supra* note 34, at 463-464.
[85] See *The FCC Fines Wireless Companies for Selling Users' Location Data*, WIRED, (2020), https://www.wired.com/story/fcc-fines-wireless-companies-selling-users-location-data/. Given the cellphones are designed to connect to the network, the only way to not be tracked would be avoid using your phone's network capabilities. Even anonymized cellphone data can be easily re-identified. See Yves-Alexandre De Montjoye et al., *Unique in the crowd: The privacy bounds of human mobility*, 3 SCI. REP. 1376 (2013).
[86] See Competition and Markets Authority, *supra* note 76, app. G, at 107-8 (explaining the shift and how it enables continued tracking despite decreases in third-party cookies).
[87] See Omri Ben-Shahar & Carl E. Schneider, *The failure of mandated disclosure*, UNIV. PA. LAW REV. 647–749 (2011), at 650-651 (describing how "mandated disclosure is ubiquitous (…) [but] not only does the empirical evidence show that mandated disclosure regularly fails in practice, but its failure is inevitable").
[88] Omri Ben-Shahar & Adam Chilton, *Simplification of privacy disclosures: an experimental test*, 45 J. LEG. STUD. S41–S67 (2016), at 4-5; See also Christine Utz et al., *(Un) informed Consent: Studying GDPR Consent Notices in the Field*, *in* PROCEEDINGS OF THE 2019 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 973–990 (2019), at 974,

they cannot address the many externalities involved in data processing.[89] Dark patterns employed in design interfaces can also greatly influence consumer decision-making, sometimes without significant awareness or pushback.[90]

Once this personal information is collected, it can behave as a public good—a non-rival, hardly excludable good that can be easily and cheaply copied and that quickly spreads through a complex web of companies and data brokers.[91] This means that once data has been shared, it is hard to purge it from this complex system. In addition, advances in computer power and mining techniques mean that companies find new uses for old data that even companies themselves did not anticipate at the time of collection.[92]

In such a context, the CCPA's and the GDPR's sophisticated disclosure and consent obligations cannot wash away the fact that mandated disclosure and other provisions aimed at increasing consumer data awareness have failed. Multiple studies have confirmed the high levels of information asymmetries and opacity in data collection and processing. The vast majority of people do not read privacy policies and do not understand data collection and processing, and simple simplification attempts have not changed that.[93] Only 29% of Americans know that

(showing how consent can be easily manipulated by dark patterns such as the position on the browser and the colors used).

[89] Omri Ben-Shahar, *Data Pollution*, 11 J. LEG. ANAL. 104–159 (2019), at 120, (describing how externalities in data collection prevent private contracting over data from being socially efficient).

[90] Jamie Liguri and Lior Strahilevitz, *Shinning a Light on Dark Patterns*, 13 J. LEG. ANAL. 43-109 (2021).

[91] Acquisti, Taylor, and Wagman, *supra* note 34, at 446 (affirming that shared personal data behaves like a public good, while one of the core tenets of data protection is to be able to exclude access to certain types of data); Englehardt and Narayanan, *supra* note 81, at 8 (finding more than 81.000 third-party tracking companies, 123 being normally found in navigation).

[92] Acquisti, Taylor, and Wagman, *supra* note 34, at 447.

[93] *Id.* at 479 ("numerous empirical studies have highlighted the limitations of transparency mechanisms [to increase data protection]).

Facebook owns Instagram and WhatsApp,[94] and only 26% understand that Facebook creates user profiles to target ads.[95] If consumers cannot grasp even the basics of the data collection network, they will not understand that when they use a cellphone app their real time location is being sold to a complex network that enables, among others, the US Federal Government to enforce immigration laws or track potential terrorist threats.[96] Uninformed consumers cannot exercise exit nor voice, undermining the role of markets as mechanisms to help promote compliance with privacy laws.

c. Market concentration further hinders exit and voice

Information asymmetries, however, provide only a partial explanation for why market solutions appear to be failing to align consumer privacy preferences. Another problem is that the economic structure of many data markets pushes them to *winner-takes-all* or *winner-takes-most* scenarios where only one or two leading companies thrive. Indeed, a range of reports from expert panels and antitrust authorities from around the world highlighted the role of network effects, large economies of scale and scope (in part due to network effects), low marginal costs and low distribution costs in inducing concentration in different data markets.[97] Many of these dynamics are connected to the crucial role data itself plays as an input to products and services of the digital economy.[98] More

[94] Pew Research Center, *Americans and Digital Knowledge* (2019), https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/.
[95] Pew Research Center, *Facebook Algorithms and Personal Data* (2019), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/.
[96] See Byron Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL STREET JOURNAL, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, MOTHERBOARD, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
[97] Lancieri and Sakowski, *supra* note 13, at 10.
[98] Michal S. Gal & Oshrit Aviv, *The competitive effects of the GDPR*, 16 J. COMPET. LAW ECON. 349–391 (2020), at 352.

importantly, these conclusions are supported by detailed analysis of particular competitive conditions in different relevant markets, including: (i) search;[99] (ii) social media;[100] (iii) search advertising;[101] (iv) display advertising;[102] (v) mobile app stores and mobile operating systems;[103] (vi) online marketplaces;[104] and (vii) mobile mapping services.[105]

In addition, concentration is growing in the infrastructure/backbone of the internet. Amazon Web Services' commands the internet cloud industry;[106] by some estimates, the Google maps API has a 90% global market share;[107] Google fonts also has a 90% market share;[108] Google tags, including Google Analytics, cover more than 80% of popular websites, while Facebook covers around 40% of the same websites.[109] These are all avenues for companies to collect consumer data. Many companies also obtain sensitive data directly from providers: Google, for example, has direct access to credit card data;[110] research indicates that 61% of mobile apps transfer data to Facebook the moment a consumer opens the app, even if the user does not have a Facebook account,[111] and

[99] Lancieri and Sakowski, *supra* note 13, at 56; Adrian Kuenzler, *Advancing Quality Competition in Big Data Markets*, 15 J. COMPET. LAW ECON. 500–537 (2020), at 515 (discussing limits on the exercise of exit and voice in search markets).
[100] Lancieri and Sakowski, *supra* note 13, at 61.
[101] *Id.* at 47
[102] *Id.* at 50.
[103] *Id.* at 37.
[104] *Id.* at 50.
[105] *Id*. at 75.
[106] *Id*. at 56.
[107] Datanyze, *Google Maps API Market Share and Competitor Report*, /market-share/mapping-and-gis--121/google-maps-api-market-share.
[108] Datanyze, *Web Fonts Market Share Report*, /market-share/web-fonts. Google Fonts is a free, open source web fonts websites use to format their websites. While Google states it does not collect data in exchange for the fonts, the control over the infrastructure allows the company to change the practice anytime.
[109] Competition and Markets Authority, *supra* note 76, app. G, at 99-100.
[110] Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales, BLOOMBERG.COM, August 30, 2018, https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.
[111] Australian Competition and Consumer Commission, *supra* note 80, at 391.

88% of Google Play Store apps transfer data back to Google.[112] For consumers to avoid the collection of personal data due to backbone concentration or Business-to-Business deals they would have to all but stop using the internet.[113]

Both the CCPA's and the GDPR's provisions on data portability are aimed at facilitating consumer exit in markets where data is a key input. However, porting the data of a single consumer at a specific point in time—what is normally allowed by data portability rights—will do little to weaken the significant market power of leading digital platforms and effectively enable consumer exit. While individual data portability may be coordinated into a larger effort that could have such power, this coordination faces a chicken-and-egg problem: competitors struggle to obtain the critical mass that would trigger a natural mass migration; and consumers' face a collective action problem to independently organize such migration. In addition, these rights to data portability usually do not include constant portability of update and accurate data, a problem for markets where data half-life is short. As such, simple data portability is unlikely to enhance consumers' exit strategies.

An alternative may be to establish a broader obligation of data interoperability—that is, the automated, constant transfer of data.[114] This solution, however, has its own important shortcomings. First, in the absence of a clear legal mandate, interoperability faces important legal hurdles. For example, US anti-hacking laws allows companies to prevent third-parties from

[112] Binns et al., *supra* note 83, at 26
[113] Gunes Acar et al., *The web never forgets: Persistent tracking mechanisms in the wild*, *in* PROCEEDINGS OF THE 2014 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 674–689 (2014)at 675, (surveying the 100.000 most popular websites in Alexa in 2014 for techniques for online tracking that cannot be stopped by users, like fingerprinting, and finding that even very sophisticated users cannot protect themselves without significant trade-offs in terms of website functionality).
[114] Lancieri and Sakowski, *supra* note 13, at 94.

accessing computerized systems and databases.[115] Second, while a legally mandated interoperability may enable consumer exit in some markets, such mandated sharing of personal data can harm personal privacy. Interoperability is complex, costly and research has shown that large bodies of anonymized personal data can be (sometimes easily) reidentified.[116] At the same time, the value of databases is in their volume and complexity and is time-sensitive. On the one hand, an interoperability system based on consent faces the same collective action challenges of data portability. On the other, a system that relies on differential privacy or other similar protocols to mandatorily share data while protecting privacy will probably be so restricted that it will not effectively promote exit.[117]

Exit and voice only function if consumers can threaten exit. However, many data markets tend to monopoly, allowing companies to impose unfavorable data collection and processing terms

[115] Facebook, for example, has previously leveraged Federal criminal law to prevent the development of a potential competitor in social networks markets called Power Ventures, whose goal was exactly to create an interoperable meta-social network.115 See Thomas Kadri, *Digital Gatekeepers*, 99 TEX. LAW REV. (2021) at 17-20

[116] Paul Ohm, *Broken promises of privacy: Responding to the surprising failure of anonymization*, 57 UCLA LAW REV. 1701 (2010), at 1716 (describing how new methods made reidentifying databases much easier); Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the success of re-identifications in incomplete datasets using generative models*, 10 NAT. COMMUN. 3069 (2019), at 2-3, (stating that "numerous supposedly anonymous datasets have recently been released and re-identified" and estimating that their model can leverage on an incomplete database of 1% of the US population to reidentify almost 90% of the population).

[117] Daniel Kifer et al., *Guidelines for Implementing and Auditing Differentially Private Systems*, ARXIV PREPR. ARXIV200204049 (2020), at 7, (describing the restricted "privacy budget" that is essential to ensure that personal data remains anonymized in Facebook's Social Sciences One project, probably the world's most advanced employment of differential privacy protocols). Effective anonymization requires restricting access to data, but this restricted access would not help promote competition.

notwithstanding consumer preferences.[118] Facebook, for one, has been condemned in both Germany and Italy for such practices.[119]

Data collection and processing is complex, but a simple example can help convey how information asymmetries and market concentration might prevent consumers from fully exercising exit and voice in data markets. To help contact and tracing programs during the Coronavirus pandemic, the UK government asked pubs to keep a record of consumers' names and cellphones. Restaurant staff then used this information to harass customers by sending messages asking them out on dates[120]—a violation of GDPR requirements such as specific consent for data processing and purpose limitation or of obligations to fully inform consumers under the CCPA. In theory, consumers can rely on markets to punish violating pubs—they can demand that management fires the harasser (voice), or they can change pubs, forcing the violating bar to go out of business (exit). However, data can be easily shared without the consumer knowledge—any restaurant staff can copy the consumer's name and telephone number and even send it to a friend for almost no cost and without awareness. If consumers provided their information to different pubs, they would not know which

[118] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 745-746. Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. LAW J. 39 (2019), at 55 and following (for a detailed report on how Facebook reflected at least some consumer privacy concerns while social media markets were competitive, but stopped doing so once Facebook dominated the market).

[119] Filippo Lancieri & Caio Mario Pereira Neto, *Designing remedies for digital markets: the interplay between antitrust and regulation, Forthcoming* JOURNAL OF COMP. LAW AND ECONOMICS (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3704763, at 17; Kerber and Zolna, *supra* note 72; Nicolo Zingales, *Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law*, 33 COMPUT. LAW SECUR. REV. 553–558 (2017).

[120] Donia Waseem & Joseph Chen, *Contact tracing: why some people are giving false contact details to bars and restaurants*, THE CONVERSATION (2020), http://theconversation.com/contact-tracing-why-some-people-are-giving-false-contact-details-to-bars-and-restaurants-143390

establishment to punish unless if revealed by the wrongdoer. Similarly, if only one pub exists in their city, consumers' have no exit options. Owners can ignore complaints and force consumers to choose between discounting the violation or stop going to pubs altogether.

As depicted in detail above, the complexity of data protection markets aggravates these information asymmetries and market concentration concerns—consumers share similar data with multiple providers without even knowing that their data is being collected, and may need to decide between sharing personal data or giving-up the use of smartphones, online search or digital mapping altogether. Under such circumstances, markets will not work as a mechanism to ensure that companies reflect consumers' privacy preferences.

ii. Torts

a. Tort liability as a complement to market forces

Tort-based statutory causes of action can complement markets in ensuring that companies account for consumers' preferences without many of the downsides of top-down, command-and-control, public regulation.

Tort liability has many virtues. It continues to directly empower consumers, allowing for decentralized, often low-cost enforcement as damages encourage users to monitor companies and bring violators to court.[121] Moreover, when coupled with fee-sharing arrangements, collective redress mechanisms such as class actions or punitive damages, tort liability can sometimes overcome problems of information asymmetries or the low value of claims. Injunctions and

[121] Peter Cane, *Tort law as regulation*, 31 COMM WORLD REV 305 (2002), at 316.

damages awards may force powerful companies—including monopolies—to internalize consumer preferences by compelling or making it unprofitable for corporations to violate the law.[122]

Data protection laws acknowledge this power, establishing/outlining statutory data-related torts that complement markets in promoting consumers' preferences. The CCPA and the GDPR, for example, grant consumers a different combination of individual rights, such as the ones to require data rectification and erasure, a right to opt-out of data sales (in California), the right to be forgotten (in the EU), a right to be notified about data breaches, the right to object to the processing of some forms of data, a right to withdraw consent, etc.[123] These are paired with general commands that consumers should be entitled to receive "full compensation" for harms suffered (GDPR) or can obtain injunctions and claim statutory damages against (at least some) violations of the law (CCPA). Because of the GDPR, citizens harassed by pub staff can complement exit and voice by going to Courts to obtain injunctions or collect damages for violations of their data protection rights.

---

[122] Ben-Shahar, *supra* note 89, at 124 (stressing how tort law can complement private contracting in implementing legal commands).

[123] Chander, Kaminski, and McGeveran, *supra* note 3, at 1752 (stressing how the GDPR and the CCPA "share, too, the core elements of a number of additional individual rights (thought they differ in the details)" and listing those rights). For the many differences, see *Id.* at 1755-62. A clarifying note is important here. While the CCPA grants users a series of rights it does not pair them with the capacity to directly enforce these rights through private rights of action (Section 1798.150(c)). For the purposes of this article, which is focused on how abstract legal rights are enforced on the ground, this separation can be understood as the law outlining a type of concrete harm that could qualify as a statutory tort (e.g. the ability to sue when a company does not grant a consumer the ability to access and correct information in databases) but removing from the consumer its independent enforcement power through the direct filing of complaints—something that greatly weakens the tort system as an effective enforcement mechanism. This separation is well explained, for example, by Justice Alito majority ruling in Spokeo: "Congress' role in identifying and elevating intangible harm does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants ta person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation." Spokeo, Inc. v. Robins, , 136 S.Ct. 1540 1549 (2016). Indeed, the potential weakness of this dynamic is exactly what this Section explores.

A reliance on statutory torts as a mechanism to enforce consumer preferences, however, faces important shortcomings. First, and importantly, torts suffer from many of the problems around information asymmetries that plague markets: if goods are so complex and opaque that consumers or their attorneys cannot identify violations or cannot prove that it took place, then torts will not work as intended.[124] In addition, torts are also plagued by agency problems in the definition of the tort[125] and Courts sometimes struggle to establish causation, calculate damages or are incapable of addressing negative externalities that go beyond the harm to a single individual.[126] Market power may also undermine torts as firms design opaquer products and leverage on their deep pockets to hire the best lawyers, conflict key economic consultants, drag-on discovery and generally raise the costs of litigation.

These shortcomings are not inevitable, they depend both on the design of the judicial system and of the statutory tort. Yet, an analysis of the GDPR and the CCPA reveals important obstacles that can prevent statutory torts from becoming an effective data protection enforcement mechanism. That is because lawmakers failed to account for how information asymmetries, market power and other general hurdles undermine data-related statutory torts when designing these laws.

---

[124] Steven Shavell, *Liability for harm versus regulation of safety*, 13 J. LEG. STUD. 357–374 (1984). at 363 (listing dispersed harms/lack of economic incentives to sue, the discovery of the harm, establishing causality and market power as barriers to effective compensation through tort liability).

[125] Torts may reflect the preferences of only a subset of consumers or even of other parties than consumers. For example, mandatory rules may lead to higher quality/higher price combinations that exclude poorer consumers. See Oren Bar-Gill & Ben Ben-Shahar, *Regulatory techniques in consumer protection: a critique of European consumer contract law*, 50 COMMON MARK. REV 109 (2013), at 113; Waldman, *supra* note 44, at 793 (describing how legal endogeneity is a problem in data protection).

[126] Ben-Shahar, *supra* note 89, at 125.

b. Information asymmetries and market power undermine the CCPA

Start with the CCPA. Tort liability has historically been a weak mechanism to safeguard consumers' data protection preferences in the US. Many US Courts refuse Article III standing or actual recovery in privacy violation/data breach lawsuits for lack of a cognizable harm.[127] Privacy class action lawsuits are normally targeted at a couple of statutes that have statutory damages, and even those face many problems around conflicts of interest between lawyers and consumers.[128] While the CCPA (and the CPRA) could have addressed these shortcomings, some of the same information asymmetries that plague exit and voice also negatively impact tort enforcement under the Act.

An effective private litigation system requires consumers to be aware that violations took place. While this may be easier in data security given that new mandatory notifications of data breaches provide consumers with a clear warning, this is not the case for rights that limit the collection and processing of personal data. If information asymmetries, opacity, and externalities prevent consumers from understanding what is being done with their data and triggering exit and voice, they also prevent them from litigating these matters.

The American class action system is structured to circumvent this problem. By grouping claims, it allows for the pooling of resources and increases the sophistication of plaintiffs, enabling the more extensive civil discovery typical of US law. However, the complexity and opacity of data markets and the market power of digital platforms also undermine data protection class actions by enabling companies to impose terms of use that minimize their liability, to design more complex interfaces that hinder characterization of harm and to generally increase the cost of litigation—not

[127] Solove and Citron, *supra* note 27, at 739, 741; Ben-Shahar, *supra* note 89, at 125.
[128] Marc Rotenberg & David Jacobs, *Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres*, *in* ENFORCING PRIVACY 307–333 (2016), at 315.

only plaintiffs must hire experts and conduct lengthy investigations to discover violations but they do so aware that their counterparty has almost endless resources to fight the claims.

Indeed, with the potential exception of the "*do not sell my data*" button, most of the CCPA's consumer data rights remain directly linked to the companies' terms of use, allowing them to draft these terms in a way that hinders or blocks tort lawsuits (for example, by allowing for widespread data collection and processing or by requiring class waivers or mandatory arbitration).[129] The designed complexity and opacity of data collection and processing mean that data harms are neither immediate nor visible[130]—making it even harder for parties to survive a motion to dismiss, certify a class or prove the causation necessary to trigger liability. In theory, the CCPA statutory damages can provide courts with guidelines for harm calculation and can become an important incentive to encourage sophisticated plaintiffs to file the expensive class action lawsuits that dominate this field. However, the CCPA's statutory damages are no panacea as: (i) they only apply to data breach litigation and not to core data protection rights like the "do not sell my data" feature; (ii) even those data breach claims are overseen by the Attorney General of California, who may take over the case or even simply block consumers from moving forward;[131] and (iii) they still require plaintiffs to prove some actual harm before they can claim the minimum damages.[132] Importantly,

---

[129] A practice that is widespread among large US companies. See Imre Stephen Szalai, *The Prevalence of Consumer Arbitration Agreements by America's Top Companies*, 52 UC DAVIS REV ONLINE 233 (2018), at 234 (finding that 81 of Fortune 100 companies used arbitration agreements with connection to consumer contracts by 2018, and 78 included class action waivers); Rotenberg and Jacobs, *supra* note 128 at 313 (discussing how limitations to class actions by class action waivers/mandated arbitration clauses have undermined data protection enforcement); Waldman, supra note 44, at 796, 812 (describing how companies can evade legal liability by modifying terms of use and relying on other forms of hollow compliance).

[130] Ben-Shahar, *supra* note 89, at 125.

[131] CCPA 1798.150(b)(3).

[132] As decided in DOE V. CHAO, 540 US 614 (2004). See Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 NYUL REV 662 (2019), at 682-683, (discussing how expectation damages and other techniques to discourage inefficient breaches in data privacy

the CPRA continues to prevent consumers from directly litigating core data protection rights—in a contradiction, both laws grants users a series of data protection rights, but then do not grant them powers to directly enforcement many of these rights in Courts.

Returning to the simple pub example from above, if consumers do not know that their name and telephone is being illegally shared nor which pub shared their data, they will not file a lawsuit. Even if consumers are aware that it was pub X that shared their information, the small value of potential claims may prevent them from litigating altogether. Courts can dismiss the lawsuit or refuse to provide damages by stating that simply receiving a text message is not a cognizable harm. The pub may also prevent the lawsuit by requiring that before consumers receive drinks they tick an "I agree" box stating, on page thirty, that the consumer consents that its name and telephone may be used for any purposes the pub sees fit; that the consumer waives rights to a class action and agrees to private arbitration to solve disputes. A (very) wealthy pub can hire the best lawyers and economic experts, drag on discovery and appeal decisions all the way to the Supreme Court as a way to further discourage lawsuits. Finally, consumers in a one-pub town may not file claims because they are fearful that the aggravated pub owner will refuse to accept them in the future.

That is a stylized example: most data collection and processing takes place in a more complex and opaquer world that is filled with intermediaries—the consumer would not receive a text message by the pub, but by a call center that bought the information from a marketing agency that bought it from the pub. Nonetheless, even this simple example showcases many important limitations of data protection torts.

---

do not accomplish their goals if breaches of data contracts are difficult to detect, prove or ascertain); Solove and Citron, *supra* note 27 (discussing important legal changes that would be necessary to increase private litigation of data breach harms).

Indeed, and reflecting these limitations, even after the CCPA entered into force, new, high-profile data protection class actions lawsuits filed in California did not rely on the Act, but rather on other legislation aimed at protecting the safety of private communications such as Federal Wiretap Act or the California Invasion of Privacy Act.[133]

c. And the GDPR

The GDPR faces different but equally important challenges. Data related tort lawsuits have historically faced larger problems in the EU than in the US—for example, while Directive 95/46 (the pre-GDPR data protection legislation) created a range of specific data protection rights, problems around standing, causality and the calculation of damages have historically prevented consumers from properly enforcing these rights.[134]

While the GDPR brings about significant improvements over the old status-quo, it also missed opportunities to spur a robust personal data-related tort litigation system in the EU.

First, concerns around information asymmetries and limited consumer awareness that plague data-related torts in general may be even more relevant under the GDPR, as European jurisdictions host fewer sophisticated intermediaries like US data privacy NGOs and class-action plaintiffs and normally lack the extensive civil discovery available in the US.[135] The GDPR enables not-for-profit bodies, organizations or associations that have been constituted specifically for this purpose

[133] See, for example, two class-action lawsuits filed against Google in July 2020, Case No. 20-3664: Brown et al v. Google LLC et al, , https://www.insurancejournal.com/app/uploads/2020/06/brown-v-google.pdf. and Case No. 3:20-cv-4688: Rodriguez et al v Google LLC et al, , https://www.classaction.org/media/rodriguez-et-al-v-google-llc-et-al.pdf.
[134] Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 93.
[135] There are some potential exceptions, like the NYOB organization founded by privacy activist Max Schrems or the La Quadrature du Net, founded by French activists. Even these, however, have limited funding. See discussion below.

to represent consumers—it is up to Member States to determine specific rules on who will have standing to file such lawsuits.[136] The Regulation also leaves some margin for discretion in terms of court selection.[137]

Details around who has the power to sue, what are the resources of these organizations, which Courts have jurisdiction and which laws are applicable are key for an effective private litigation system: there is a vast scholarship in the US about strategic litigation and preclusion in class action lawsuits[138] and these strategies are known to preclude effective enforcement of data protection rights in the country.[139] EU consumers have stronger protections against the strategic use of jurisdiction, arbitration and class action waivers.[140] However, until the system is fully in place—including the passage and effective implementation of the much discussed EU Collective Redress Directive—the risks of abuse remain.

Another potential drawback is in the calculation of damages. The GDPR establishes that persons should be compensated for "material and non-material damages" arising from privacy

[136] GDPR, Art. 80 and recital 142.
[137] GDPR Art. 79 establishes that the lawsuit may be filed before the Courts of the Member State where the company is established or where the consumer resides. Art. 81 and recital 144 establish that when Courts identify multiple proceedings based on a similar fact pattern, parties may request that cases are consolidated by the Court where the first complaint was filed.
[138] Tobias Barrington Wolff, *Preclusion in Class Action Litigation*, 105 COLUM REV 717 (2005) at 746 (discussing conflicts of interest in plaintiff counsels in rapidly securing settlements that preclude the class in exchange for generous fees).
[139] Rotenberg and Jacobs, *supra* note 128, at 316 (providing examples of this problem).
[140] Julian Nowag & Liisa Tarkkila, *How much effectiveness for the EU Damages Directive? On the EU Damages Directive and Contractual Clauses Hindering Antitrust Damages*, 57 COMMON MARK. LAW REV. (2020), at 466, (exploring how the Brussels Regulation and the Unfair Contract Terms Directive protect consumers against contractual clauses establishing mandatory jurisdiction, arbitration and/or denying participation in class actions when these impact the effectiveness of EU laws).

violations.[141] The problem is that the case-law of the European Court of Justice in this area is sparse.[142] Here, again, information asymmetries associated with the complexity and opacity of data protection make it harder for consumers to prove standing, demonstrate causation or calculate damages, undermining the tort system. Some scholars have stressed how private litigation under the GDPR may face at least three important hurdles: (i) identifying who is the controller of the information; (ii) demonstrating the performance of an illegal act by the controller; and, in particular (iii) demonstrating causality between the processing of the personal data and damages to the individual involved.[143]

Company's economic power and their associated deep pockets is also another barrier. For example, a previous study on the lack of private litigation under the preceding Directive 95/46 indicated not only that consumers were unaware of most violations, but also that they feared punishment by the large companies that they relied on if they filed complaints.[144] If consumers cannot credibly threaten to file complaints, tort liability will not force companies to comply with their preferences. Data privacy litigation is also bound to be expensive, as lawsuits might involve significant market monitoring, technical preparation and discovery to ascertain when companies' opaque data practices are illegal. Unless national laws or European courts award meaningful material and non-

[141] GDPR, Art. 82. Recital 146 complements it by establishing that "the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation".
[142] Johanna Chamberlain & Jane Reichel, *The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation*, 89 MISS LJ (2020), at 8, (stressing how the ECJ has not decided any case on Article 82 and that it will be up to specific Member State law to ensure that the broad principle is indeed effective).
[143] Brendan Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 J INTELL PROP INFO TECH ELEC COM L 271 (2016), at 275; 283 (describing the problems in assessing civil liability in Directive 95/46 and stressing how the GDPR might help by shifting the burden of proof after a demonstration of prima facie harm).
[144] Golla, *supra* note 42 at 72.

material damages for data protection violations, private litigation may not be worth the cost.[145] However, the GDPR does not require minimum statutory damages, punitive damages or other forms of increased compensation that can encourage sophisticated intermediaries to start costly investigations and/or file lawsuits—it will be up for member states to establish the value of potential damages.

Ultimately, there is a reasonable risk that the GDPR private litigation system is structured similarly to the European antitrust private litigation system, where the bulk of lawsuits takes place only *after* the government had found undertakings to be in violation of antitrust laws.[146] Moreover, the EU Damages Directive for competition law violations has so far failed to spur consumer-driven private litigation, which remains largely nonexistent. These are bad omens for the success of GDPR private litigation, as not only is antitrust a more mature enforcement system but the consumer-to-business nature of data protection laws limits company-driven litigation. Indeed, whenever European online privacy NGOs discover violations, they usually file complaints before EU regulators rather than suing companies in Courts—showcasing the weakness of the tort system.[147]

Tort liability as a mechanism to promote legal compliance will certainly be weaker in a system where private parties are subordinated to regulators than in one relying on mixed public/private litigation. That is because on this subsidiary system the enforcement of legal rights is no longer decentralized and directly in the hands of consumers, but rather in the hands of government regulators. As a result, tort liability risks becoming merely a way to increase the deterrence value

---

[145] Nowag and Tarkkila, *supra* note 140, at 472 (stressing how the small value of awards is an impediment to EU consumer antitrust lawsuits).
[146] *Id.* at 457 (stressing how follow-on antitrust claims are likely the most common in the EU).
[147] Nicholas Vinocur, *'We have a huge problem': European regulator despairs over lack of enforcement*, POLITICO, December 27, 2019, https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/ (describing how EU privacy advocates have been filing complaints before regulators, not courts).

of public fines, not the independent enforcement mechanism it initially was. Moreover, as tort liability gets closer to regulatory enforcement, it incorporates the virtues and shortcomings of public regulation—the topic of the next section.

iii. Regulatory enforcement

a. Command-and-control regulation as a third enforcement mechanism

The use of the government's coercive or fining powers to enforce command-and-control regulations is a third, important mechanism to ensure that markets reflect consumer preferences.[148] Regulatory enforcement represents a decision by governments to remove consumers from the direct determination of quality/prices in markets, replacing them by commands that impose specific obligations, minimum levels of quality, maximum prices, etc. In essence, regulatory enforcement is the combination of three components: (i) setting standards of behavior; (ii) monitoring compliance with those standards; and (iii) enforcing the standards against non-compliers.[149] All three are non-trivial, so governments create bureaucracies dedicated to fulfilling these tasks. Regulators issue rules, conduct investigations, order companies to change behavior and impose fines to force even the largest businesses to comply with the legal/regulatory commands.[150]

Online privacy laws have long relied on regulators as complementors to markets and torts to ensure that companies reflect consumer preferences.[151] Newer laws further strengthened public

[148] Shavell, *supra* note 124, at 373; Kuenzler, supra note 70, at 18-19.
[149] Cane, *supra* note 121, at 312.
[150] *Id.* at 317.
[151] Directive 95/46 required EU Member State to establish independent data protection authorities and the FTC has concluded hundreds of settlements with companies for legal violations. See Solove and Hartzog, *supra* note 23, at 628 (analyzing 154 FTC privacy complaints, a number that has only increased since the article was published in 2013).

enforcement: both the GDPR and the CCPA require public authorities to define the content of many data protection rights and effectively enforce those rights.[152] The newly passed CPRA brings California closer to the EU with the creation of the California Privacy Protection Agency, an independent public bureaucracy responsible for enforcing the CCPA as of January 2023. All of these agencies are granted powers to order companies to change their behavior and impose billions of dollars in fines for non-compliance.

The option for public regulation, however, leads to important changes that can negatively impact enforcement dynamics. Two are noteworthy: First, the enforcement system now faces two agency problems, not only consumers lose their power to establish the content of regulations (as in torts) but they also lose control over when to enforce violations (a governmental employee has discretion to decide when to take action). This opens new avenues for regulatory capture, or conflicts of interest between governments (agents) and consumer (principals). Second, the centralization of monitoring and enforcement increases administrative costs and risks that the system is under-resourced, as governments may refuse to fund the costly and complex bureaucracies necessary to properly enforce the regulations.

These two problems are common to regulatory regimes and can be mitigated through clever institutional design. However, the large information asymmetries and market power that characterize many data markets significantly exacerbates them. Indeed, the regulatory systems created through the GDPR and the CCPA lack different but important institutional solutions that could help alleviate concerns.

[152] Chander, Kaminski, and McGeveran, *supra* note 3, at 1759-61 (comparing the role of regulators in both laws).

b. The risks of regulatory capture in data protection

George Stigler's Nobel Prize winning insight was that regulators' and consumers' preferences may misalign, so that governmental action could protect companies and make consumers worse off. For Stigler, one of the main drivers of regulation is the demand by private, politically powerful interest groups trying to appropriate economic rents.[153] Effective governmental capture, however, is not easy, not least because it requires coordination among industry members who have private incentives to defect or to free ride.[154] The scholarship on regulatory capture has evolved significantly since Stigler wrote his groundbreaking piece.[155] While main important gaps still remain, we now better understand how agents must expend significant political capital to influence regulation, relying on multiple mechanisms such as cash payments, revolving doors, shaping of the public discourse through control over the media and over academia, the ability to mobilize stakeholders and control over the human capital required by regulators.[156] Most capture does not take place through direct payments to corrupt bureaucrats. Rather, it relies on a long process of persuasion, in which industry players benefit from information asymmetries and constant interaction, pay consultants and academics and strategically use revolving doors to convince the

[153] Richard A. Posner, *Theories of Economic Regulation*, 5 BELL J. ECON. MANAG. SCI. 335–358 (1974), at 335, 343; George J. Stigler, *The theory of economic regulation*, BELL J. ECON. MANAG. SCI. 3–21 (1971), at 5-7.
[154] Posner, *supra* note 153, at 346; Stigler, *supra* note 153, at 7, 12.
[155] See, generally, Christopher Carrigan & Cary Coglianese, George J. Stigler,'The Theory of Economic Regulation', in THE OXFORD HANDBOOK OF CLASSICS IN PUBLIC POLICY AND ADMINISTRATION (2015); Sam Peltzman, *Stigler's Theory of Economic Regulation After Fifty Years*,https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3785342 (2021). Andrei Shleifer, George Stigler's Paper on Regulation and the Rise of Political Economy, PROMARKET (2021), https://promarket.org/2021/04/28/george-stiglers-regulation-political-economy-capture/
[156] Luigi Zingales, *Towards a political theory of the firm*, 31 J. ECON. PERSPECT. 113–30 (2017), at 122, 126; Luigi Zingales, *Preventing Economists Capture*, *in* PREVENTING REGULATORY CAPTURE: SPECIAL INTEREST INFLUENCE AND HOW TO LIMIT IT (2013).

authorities that some specific form of regulation that protects the company is actually in the public interest.

Scholars identified key market characteristics that encourage private capture: (i) the concentration within the industry and the alignment of interests between players (that helps overcome collective action problems); (ii) opacity and information asymmetries between the industry and regulators; (iii) how dispersed the group paying the rent is; (iv) how opaque the rent payment is; and (v) the salience of the topic for the general public.[157] Importantly, this literature indicates that capture is *possible*, not that it *always happens*—the risk increases as the specific industry aligns with the characteristics described above.[158] Political influence is always a matter of degree, and different regulations may well reflect different combinations of public and private interests.

c. Information asymmetries and market power increase the risks of capture in data protection

The large information asymmetries and market power found in data markets increase risks of private capture of these new public enforcement systems. As discussed above, many key data markets are concentrated around a handful of players who usually share preferences in favor of extensive data collection.[159] In addition, rent payments in online privacy are both obscure and

[157] Zingales, *supra* note 156, at 116-119; Carrigan and Coglianese, *supra* note 155, at 3.
[158] Stigler, *supra* note 153, at 10. Carrigan and Coglianese, *supra* note 155, at 7. The cost of exercising political power against the community increases the more the capture damages the community through rent extraction or the easier it is for the community to organize to defend its interests through civil rights associations, universities, the media, etc.
[159] See Part II.A.3 above. The potential exception is Apple. However, even Apple has been criticized for recurrently putting profits above privacy, such as when the company accepts billions of dollars from Google to secure the default search engine position on Safari—ignoring privacy-friendly alternatives such as DuckDuckGo—or its willingness to share private data as a condition to operate in countries such as China and Russia. It is also being sued for GDPR violations. See Ian Bogost, *Apple's Empty Grandstanding About Privacy*, THE ATLANTIC (2019), https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/; Natasha Lomas, *Apple's IDFA gets targeted in strategic EU privacy*

distributed: data collection is complex, often occurs in the background of regular product/service use and replication and distribution costs are marginal, so consumers—a heterogeneous and disorganized group—are usually unaware that they are giving up personal data. Finally, understanding the role of data in these industries also requires a particular set of technical skills that is in high demand. Governments, therefore, compete for talent with a profitable, high-paying industry, risking that revolving doors undermine enforcement and that regulatory agencies lack the technical personnel to design an effective data protection regime—the latter has already been documented in the EU.[160]

The same characteristics also increase the risk of *public* regulatory capture. Governments and citizens have some conflicting priorities in terms of data protection when criminal prosecution, national security and industrial policy are involved. Intelligence agencies' surveillance apparatus rely on the processing of personal data (e.g. communications, location, bank transfers), so that limitations on data collection also mean limitations on how successful these agencies are in doing their work.[161] Both the CCPA and the GDPR, for example, explicitly exempt criminal enforcement and national security from their application[162] and law enforcement authorities are attacking end-to-end encryption in social networks, undermining one of the most important online privacy

complaints, TECHCRUNCH, November 16, 2020, https://social.techcrunch.com/2020/11/16/apples-idfa-gets-targeted-in-strategic-eu-privacy-complaints/.) Ultimately, Apple may not have incentives to advocate for strong, industry-wide data protection standards, as that would weaken its commercial strategy.

[160] Brave, *supra* note 9, at 3, 6 (finding that almost all EU data protection agencies lack data scientists).

[161] As Richard Posner summarized, "privacy is the terrorist's best friend", Richard A. Posner, *Privacy, surveillance, and law*, 75 UNIV. CHIC. LAW REV. 245–260 (2008), at 251.

[162] CCPA Section 1798.145; GDPR art. 23.

conquests of the past decade.[163] Three out of five Commissioners of the newly created Brazilian data protection agency are members of the Brazilian armed forces.[164]

These conflicting interests in data protection are not solely restricted to technical matters such as encryption but include the broader organization of the industry. It is reasonable to assume that governments prefer fulfilling their data access needs by tapping just a handful of companies with large, comprehensive databases, rather than having to access many smaller providers. Large, centralized databases are more reliable, help increase the secrecy of the operations—only one backdoor is needed—and are better for future Artificial Intelligence applications.[165] Governments also likely prefer to concentrate compliance in a single company established in their jurisdiction than in multiple companies based abroad.

The growing economic importance of digital markets pushes for an equally expanded interconnection between industrial and data policy, which is exacerbated by the market power of some large digital companies.[166] The more personal and non-personal data are key inputs for

---

[163] Robert McMillan and Jeff Volz, *Barr Presses Facebook on Encryption, Setting Up Clash Over Privacy*, WALL STREET JOURNAL, October 4, 2019, https://www.wsj.com/articles/attorney-general-calls-on-facebook-to-limit-message-encryption-plans-11570130636.

[164] Angelica Mari, *Military takes over Brazil's National Data Protection Authority*, ZDNET (2020), https://www.zdnet.com/article/military-takes-over-brazils-national-data-protection-authority/

[165] Dakota Foster & Zachary Arnold, *Antitrust and Artificial Intelligence: How Breaking Up Big Tech Could Affect the Pentagon's Access to AI* (2020), at 13, 15, 20 (arguing that "data is a core ingredient in AI development" that bolsters national security, that data protection requirements like "siloed" data can hinder AI innovation and that the potential break-up of large tech companies can negatively impact national security by reducing network effects and deconcentrating data sources necessary for critical AI developments).

[166] China, for example, explicitly combines data and industrial policy to promote their national companies in general and in AI in particular (Hung Tran, *Industrial Policy War - Capitalism with Chinese Characteristics*, FINANCIAL TIMES, September 21, 2019, https://www.ft.com/content/79b242e2-3d21-3bcc-8880-59e6f34e96c4.); in the US, whenever companies like Facebook are faced with potential new regulation, they mention the risk that such protections may displace them in the race against China (Josh Constine, *Facebook's regulation dodge: Let us, or China will*, TECHCRUNCH (2019),

technological development in the digital era, the more governments concerned with the promotion of national champions will want to increase rather than restrict access to data.[167] This means that governments may have important economic incentives to undermine data protection enforcement by inducing market concentration, data concentration or more widespread data collection and processing.

Finally, effective data protection may increase the market power of dominant digital platforms, worsening these dynamics. This is not only due to increased compliance costs, but also because legislation both restricts access to data and concentrates the remaining data in large providers.[168] While access to a large, updated database is key in many digital markets, data protection laws have a general goal of limiting data collection and processing—disproportionately impacting smaller companies with limited direct interaction with consumers.[169] It is too early to pass a definitive judgment, but different studies have found that some side effects of the enactment of the GDPR has been increased data and market concentration.[170] What is particular about this data

---

https://social.techcrunch.com/2019/07/17/facebook-or-china/). The EU recently joined the fray, with its new "European Strategy for Data" data is predicated on data sharing and the promotion of national players. European Commission, *A European Strategy For Data* (2020), https://ec.europa.eu/digital-single-market/en/european-strategy-data

[167] Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY LAW REV. 639–694 (2013), at 666-667 (stressing how the absence of strong privacy laws was key for the development of internet innovation and the silicon valley). As Facebook's head of Global Affairs stated when pressed about data protection in an interview: "We don't hear so much about China, which combines astonishing ingenuity with the ability to process data on a vast scale without the legal and regulatory constraints on privacy and data protection that we require on both sides of the Atlantic". Constine, *supra* note 166.

[168] Gal and Aviv, *supra* note 98, at 4 ("identifying seven main parallel and cumulative market dynamics [following the GDPR] that may limit competition and increase market concentration").

[169] *Id.* at 28.

[170] Christian Peukert et al., *European Privacy Law and Global Markets for Data*, 1 CENT. LAW ECON. WORK. PAP. SER. (2020), at 11; 19; Konstantinos Solomos et al., *Clash of the trackers: measuring the evolution of the online tracking ecosystem*, ARXIV PREPR. ARXIV190712860 (2019), at 3, 6, 8 (generally find that Google gained or maintained very high-levels of market share after coming into force of the GDPR); Garrett Johnson, Scott Shriver & Samuel Goldberg,

protection/concentration dynamic is that industry players may leverage data protection regulations to protect their dominant position by complying with the law.[171] For example, both Google,[172] Facebook[173] and Apple[174] announced a series of changes to promote or to comply with data protection laws that strengthened their grip on data vis-à-vis potential competitors. Facebook has also previously leveraged access to its databases to prevent the development of competitors, potentially in violation of antitrust laws.[175] Many companies are in a data race, and while these changes are welcome from an online privacy perspective, they further increase data-related barriers to entry. Stronger, more dominant companies are better resourced to capture regulators and can more convincingly argue that they are essential to national economies.

Privacy & market concentration: Intended & unintended consequences of the GDPR (2020), at 21-22 (finding that that the GDPR led to an average increase of 17% in market concentration). There is also suggestive evidence that the GDPR led to an almost 31% decrease in the funding of data-intensive startups in Europe vis-à-vis the US (Jian Jia, Ginger Zhe Jin & Liad Wangman, *The short-run effects of GDPR on technology venture investment* (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912, at 6).

[171] Inge Graef, Damian Clifford & Peggy Valcke, *Fairness and enforcement: bridging competition, data protection and consumer law*, 8 INT. DATA PRIV. LAW 200–223 (2018). at 220-22.

[172] By dropping third-party cookies support in the Chrome browser; limiting the use of double-click IDs that advertisers use for independent monitoring of online ads and restricting third-party access to contextual data. James Hercher, *How We Got Here: A Look Back At The Privacy Changes That Reshaped Google*, ADEXCHANGER (2019), https://www.adexchanger.com/online-advertising/how-we-got-here-a-look-back-at-the-privacy-changes-that-reshaped-google/.

[173] This took place both in 2015 when Facebook restricted third-party access to users' data, and more recently when the company announced a pivot to a "privacy-centered platform"—not one that collects less data, but one that shares as little data as possible with third-parties. Josh Constine, *Facebook Is Shutting Down Its API For Giving Your Friends' Data To Apps*, TECHCRUNCH (2015), https://social.techcrunch.com/2015/04/28/facebook-api-shut-down/. and Ben Thompson, *Facebook's Privacy Cake*, STRATECHERY BY BEN THOMPSON (2019), https://stratechery.com/2019/facebooks-privacy-cake/.

[174] Why Apple's anti-tracking move hurts everyone … but Apple, VENTUREBEAT (2020), https://venturebeat.com/2020/09/12/why-apples-anti-tracking-move-hurts-everyone-but-apple/

[175] Liza Lovdahl Gormsen & Jose Tomas Llanos, *Facebook's Anticompetitive Lean in Strategies* (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400204, at 68.

Capture is always hard to identify, but there is growing anecdotal evidence suggesting it has already taken place in online privacy. Professor Waldman has aptly described how privacy laws in the US and the EU are undergoing a process of legal endogeneity that is highly deferential to industry practice, so that regulated agents define what the law means rather than the law constraining what private entities can do.[176] This prevents privacy laws from actually achieving their substantive goals. In the US, there have been multiple reports about how the FTC has been incapable or unwilling to stand up to large tech companies, including by FTC commissioners themselves.[177] In the EU, the European Court of Justice (ECJ) has been a leading EU institution in helping promote citizens' data protection rights by striking down what it saw as faulty public regulations that did not adequately promoted data protection.[178] The ECJ has also previously ruled

[176] Waldman, *supra* note 44, at 776-77, 792, 816-19.

[177] William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ REV 959 (2016), at 1011 (describing criticism of an early Facebook settlement with the FTC). Facebook's stock went up after its 2019 settlement with the FTC, hardly a sign of strong enforcement. Nilay Patel, *Facebook's $5 billion FTC fine is an embarrassing joke*, THE VERGE, 2019, https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke. A review of the FTC's enforcement actions by the Government Accountability Office concluded that all but a handful cases ended up in settlements and recommended more forceful action by a stronger regulator. United States Government Accountability Office, *supra* note 72, at 37. Two FTC commissioners dissented from a 2019 settlement with Google, one claiming that the settlement was below Google's profits with the illegal practice. Rohit Chopra, *DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA In the Matter of Google LLC and YouTube LLC* (2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf.

[178] The decision invalidating the EU-US Safe Harbor was grounded on the fact that regulators did not comply with express legal obligations to monitor transatlantic data transfers, allowing the industry to freely collect and transfer personal data, and the subsequent invalidation of Privacy Shield also affirmed that the European Commission failed to assess whether the data of European citizens would receive adequate protection if transferred to the US. Case C-362/14 - Maximilian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (2015). paras. 88-90; Case C-311/18 - Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2020:559 (2020). paras 184-185, 191.

that EU countries have not safeguarded the independence of their data protection authorities.[179] Other studies have shown that data authorities are reluctant to impose sanctions for violations, preferring to rely on cooperation[180] and, more recently European governments have been accused of using COVID to suspend GDPR rights[181] and of using the GDPR itself as a way to diminish public accountability.[182] There are many complaints from European activists and even other EU regulators that the Irish data protection authority—the leading GDPR enforcer—is dragging its feet on the enforcement of the Regulation because of the importance digital markets to the Irish economy.[183] Facebook famously settled in Ireland partially because of its "favorable regulatory reputation"[184] and NYOB, a leading European privacy NGO, has published a scathing letter accusing the Irish regulator of being "structurally biased", cooperating with Facebook to purposefully delay the enforcement of the GDPR as a way to help attract foreign investment.[185]

---

[179] C-288/12 - Commission v Hungary, ECLI:EU:C:2014:237 (2014); C-614/10 - Commission v Austria, ECLI:EU:C:2012:631 (2012) .
[180] Golla, *supra* note 42, at 73.
[181] Many European governments set-aside data protection concerns in the fight against COVID-19, with Hungary going as far as suspending the applicability of GDPR rights. See Samuel Stolton, *EU data watchdog "very worried" by Hungary's GDPR suspension*, (2020), https://www.euractiv.com/section/data-protection/news/eu-data-watchdog-very-worried-by-hungarys-gdpr-suspension/.
[182] European countries such as Hungary, Poland, Romania and Slovakia have apparently attempted to use the GDPR to harass journalists and NGOs revealing government wrong-doing. See AccessNow, *Two years under the GDPR: an implementation progress report* (2020), https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf, at 17-18.
[183] Nicholas Vinocur, *One Country Blocks the World on Data Privacy*, POLITICO (2019), https://www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/.; Vinocur, *supra* note 147; Nicole Kobie, *Germany says GDPR could collapse as Ireland dallies on big fines*, WIRED UK, 2020, https://www.wired.co.uk/article/gdpr-fines-google-facebook.
[184] Karlin Lillington, *Ireland's regulatory reputation encouraged Facebook HQ*, THE IRISH TIMES, September 9, 2015, https://www.irishtimes.com/business/technology/ireland-s-regulatory-reputation-encouraged-facebook-hq-1.2279283.
[185] NYOB, *Open Letter on the Irish Data Protection Commission* (2020), https://noyb.eu/sites/default/files/2020-05/Open%20Letter_noyb_GDPR.pdf., at 3; NYOB is also suing the Irish Data Protection Authority for the same reasons (NYOB, *Irish High Court allows*

Indeed, the lack of appropriate resources and initiative by Irish regulators has been denounced even by other European data privacy regulators,[186] leading commentators to claim that Ireland is a "safe haven for tech giants".[187]

d. The systems lacks appropriate counterweights

While capture is a constant threat to regulatory systems, the discussion above showcases how a somewhat exceptional combination of market concentration, complexity and obscurity, consumer dispersion and the strategic nature of data exacerbates its possibility in online privacy. Yet, the regulatory systems put in place by the GDPR and the CCPA lack institutional counterweights that can help fend off undue influences, such as civil oversight, lawsuits for failure to act and competition in enforcement.

Start with civil oversight. As Louis Brandeis rightly stated, "sunshine is the best of disinfectants" when it comes to fighting powerful, vested interests.[188] Data protection is certainly on the spotlight in Europe and, to a lesser extent, in the US. It is possible, then, to design regulatory systems that leverage on this public awareness to offset capture risks. However, data protection agencies in the EU and the US tend to be extremely opaque. The FTC and the California Office of the Attorney General have almost no public information about ongoing investigations. They also hardly supply information on the reasons behind the opening or closing of cases. Similarly, many important EU authorities rely on annual reports, press releases or brief statements to announce the opening or closing of investigations. In particular, many have complained about the obscurity of the Irish and

---

Judicial Review to stop Facebook EU-US transfers, NOYB.EU (2020), https://noyb.eu/en/irish-high-court-allows-judicial-review-stop-facebook-eu-us-transfers)

[186] Kobie, *supra* note 183.

[187] AccessNow, *supra* note 182, at 14.

[188] LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT - CHAPTER V: WHAT PUBLICITY CAN DO (1914), https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-chapter-v

Luxembourg data authorities, probably the EU's most powerful.[189] The Irish Data Protection Commission, for example, does not host even basic transparency mechanisms such as a page summarizing the status of ongoing cases or a public agenda for officials.[190] As seen above, European privacy NGOs accused the agency of holding numerous confidential meetings with defendants to advise them on how to comply with the law, withholding most of the information from complainants and from other European regulators.[191] Without transparency there cannot be an effective civil oversight of the Government.

Lawsuits for failure to act are another important mechanism in the fight against private capture.[192] In this area, the GDPR is more advanced than the CCPA, requiring that authorities investigate complaints filed by data subjects, inform them of the status of their complaints after three months of the filing and allow private parties to file complaints against regulators in case of breach of this obligation[193]—the CCPA (even after CPRA amendments) has no similar provisions. Even the GDPR, however, has important flaws connected with the lack of agency transparency and the fact that regulators retain wide discretion in deciding how to handle complaints—there is minimum judicial oversight[194]—allowing agencies to potentially game provisions and delay cases indefinitely.[195]

---

[189] Vinocur, *supra* note 147.
[190] As of May 9, 2021.
[191] NYOB, *supra* note 185, at 8-9.
[192] The best example being the SCHREMS I, *supra* note 178, and SCHREMS II, *supra* note 178, cases referenced above.
[193] GDPR Arts. 57(1)(f) and 78(2).
[194] David Erdos, *Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?* (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521372, at 6.
[195] Authorities can simply provide an update that the cases are ongoing, delaying them indefinitely. This seems to have happened in the UK, where the First-Tier Tribunal decided at least six cases claiming that users only have a right to object against well-defined procedural violations, not the final outcome of cases. See *Id.* at 8 (quoting Platts v Information

Finally, regulatory systems must always thread a fine balance between relying on a single, powerful regulator with the appropriate powers and resources to challenge dominant businesses and creating overlapping enforcement powers, multiplying the number of agents a party has to influence to determine the final outcome of a policy. The GDPR and the CCPA/CPRA adopt different strategies: while the Californian law concentrates all enforcement of non-data breach violations in the California State Attorney General (or, later, the California Privacy Protection Agency), the GDPR foresees enforcement by multiple national data protection authorities and enables "joint investigations" between these agencies as a way to solve potential disputes. While this European dispersion of enforcement power may be welcome as a mechanism to increase accountability, the creation by the GDPR of a one-stop shop system reliant on a "lead supervisory authority"[196] combined with a convoluted system of joint-investigations[197] effectively concentrates key EU data protection enforcement in two regulators located in Ireland and Luxembourg[198]—countries that are particularly prone to regulatory capture as they disproportionately benefit from the growth of the digital economy.[199] This is a serious institutional design flaw that all but nullifies

Commissioner [2019] UKFTT 2018/0211 (GRC) and Shiel v Information Commissioner [2019] UKFTT 2019/0018 (GRC)).

[196] GDPR Art. 56(1)

[197] In GDPR joint investigations, a lead authority can either invite others to a joint investigation or non-lead authorities may request the European Data Protection Board ("EDPB") to include them in an investigation. If a conflict between the authorities takes place, the decision by the lead authority prevails unless 2/3 of the 29 members of the EDPB vote otherwise. Even then, the initial lead authority is in charge of adopting the final decision based on the vote (GDPR Arts. 62 and 65).

[198] Erdos, *supra* note 68, at 3. AccessNow, *supra* note 182, at 13.

[199] For example, the Irish fast growing digital sector responds for 13% of national GDP, 26% of exports and 10% of all employment. Irish Business and Employers Confederation, *Brexit and the Irish Technology Sector* (2019), https://www.technology-ireland.ie/Sectors/TI/TI.nsf/vPages/Influence~Working_Groups~data-working-group/$file/TI+Brexit+Impact+Report+WEB.pdf, at 13, 15. As mentioned above, Facebook's Deputy Chief Privacy Officer famously stated that Ireland's "regulatory reputation" is a key reason why the company is based there. Lillington, *supra* note 184.

the benefits of the multiple enforcer system, as shown by early data indicating that this cooperation mechanism has been ineffective in allowing for effective multi-party investigations[200] and by the widespread denouncing of the Irish authorities as structurally biased against GDPR enforcement.

e. Data authorities are under a heightened risk of being chronically underfunded

A second key shortcoming of a system over-reliant on public enforcement is the potential lack of resources.[201] While this risk is pervasive to all governmental regulations, data protection's distinctive combination of large information asymmetries, market power and broad applicability place data authorities under a heightened risk of being chronically underfunded.

The GDPR was partially designed to bring data protection closer to antitrust in terms of enforcement resources, fining capacity and others.[202] Antitrust and data protection policies share significant concerns around information asymmetries—both competition and online privacy violations are mostly hidden from the public view.[203] Unlike antitrust, however, data protection laws are not (mostly) targeted at a small subset of corporations that possess market power. Rather, they establish a range of complex rights and obligations that apply economy-wide: to small and large businesses, non-profit organizations and even individuals.[204] Small, unknown companies can

[200] Erdos, *supra* note 68, at 4. Most authorities have no budget or staff for joint-investigations.
[201] Shavell, *supra* note 124, at 364 (identifying high administrative costs as a key hurdle to the effectiveness of public regulation).
[202] Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 67, 92.
[203] In antitrust policy many violations take place when companies secretly collude to raise prices, one dominant company redesigns a specific product or contract to exclude a competitor or when companies in specific sectors merge.
[204] GDPR Art. 4(2); Inge Graef & Sean Van Berlo, *Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility*, EUR. J. RISK REGUL. 1–25 (2020), at 18-19 (stressing how this risks underenforcement in data protection and proposing that regulators privilege actions against large firms).

collect and process a significant amount of sensitive personal data—Cambridge Analytica being just one example—and, as the digital economy grows, the jurisdiction of data protection authorities will expand, risking that these agents become regulators of a "law of everything".[205] The FTC, for example, pursued a cellphone flashlight app for online privacy violations; the Austrian data protection authority fined a kebab shop for installing a security camera that also covered the public street and the Spanish authority issued a warning to a secondary school student who recorded and posted a video of another minor on Instagram.[206]

Data collection's ubiquitous, opaque, complex and multi-player nature significantly decreases the likelihood that these violations will be exposed. In addition, data protection regulatory regimes lack institutional design solutions that can help diminish information asymmetries and the cost of detecting violations. For example, antitrust regimes acknowledged that obscurity and complexity hindered enforcement, leading jurisdictions around the world to reform their competition laws to incorporate leniency regimes and mandatory merger notifications as a way to force/encourage private parties to supply regulators with hard-to-access information.[207] Extensive discovery rights and treble damages further encourage private parties to oversee markets and bring violators to court, increasing the overall resources dedicated to the discovery illegal behavior. The CCPA (even

---

[205] Nadezhda Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, 10 LAW INNOV. TECHNOL. 40–81 (2018).
[206] Federal Trade Commission, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers* (2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived; Muzayen Al-Youssef, *Bislang vier Strafen wegen DSGVO-Verstößen seit Mai*, DER STANDARD, November 23, 2018, https://www.derstandard.de/story/2000092017999/erst-vier-strafen-wegen-dsgvo-seit-mai.; AEPD case PS/00408/2020, published on 04/30/2021, https://gdprhub.eu/index.php?title=AEPD_-_PS/00408/2020&mtc=today
[207] See, for example, OECD, *Recommendation of the Council concerning Effective Action against Hard Core Cartels* (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0452, at 6, (recommending the establishment of leniency programs that encourage self-reporting of violations as a backbone of an effective cartel detection system).

after amended by the CPRA) and the GDPR do not incorporate any similar mandatory "information revealing" solutions in their regimes.

This somewhat unique combination of a broad mandate, a system not designed to generate the type of information required for regulatory oversight and a lack of a complementary civil society puts significant pressure on the resources data authorities need to properly perform their role. Another comparison with antitrust can help showcase the size of the challenge. European data protection agencies have grown significantly since the enactment of the GDPR: The Irish Data Protection Commission grew from 35 to 140 personnel between 2016 and 2020; the 700 staff of the UK's Information Commissioner is now larger than the antitrust division of the FTC.[208] Yet, their workload is all but endless: it took European data protection agencies only 18 months to issue the same amount of EU-wide potential cooperation requests that their antitrust counterparts issued in more than fourteen years (around 2500 investigations);[209] in the first nine months of GDPR enforcement, European data protection authorities received 206.326 notifications of potential violations, closing 37.900 investigations.[210] by November 2019, the number of complaints rose to 275.000—a potential backlog of hundreds of thousands of cases—leading to only 785 fines, most

[208] Irish Data Protection Commission, *Annual Report - 2019* (2020), https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf, at 8; UK ICO, *Information Commissioner's Annual Report and Financial Statements 2018-19* (2019), https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, at 46.

[209] Between May 2004 and December 2018, European competition authorities notified the European Competition Network about the opening of 2525 antitrust investigations, while European data authorities issued 2542 cooperation requests in just eighteen months. See Commission, *ECN - Statistics*, https://ec.europa.eu/competition/ecn/statistics.html and European Data Protection Board, *2019 Annual Report* (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2019_en.pdf. at 5, 30.

[210] European Data Protection Board, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities* (2019), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf, at 12.

still subject to judicial review.[211] Authorities themselves acknowledged they are overwhelmed with the workload.[212]

As a result, governments must continue to devote a growing share of scarce public funds to an area they might rather not, as enforcing data protection laws can conflict with some other important priorities such as national security or industrial policy. Lack of political will means that agencies may be chronically underfunded. For example, the 2019 budget of the California office of the Attorney General, which is responsible for overseeing the CCPA, was around USD 5 million, enough only to support an enforcement staff of 23 lawyers who are also responsible for broader consumer protection.[213] The FTC has acknowledged that lack of resources is undermining its enforcement capacity[214] and prevents the expansion of the agency's 46-person strong data protection team (4% of the agency's total staffing), which had been criticized as insufficient to effectively monitor and enforce data protection laws.[215] Yet, the FTC's annual budget is around USD 330 million, while the guaranteed funding of the California Privacy Protection Agency is only USD 10 million;[216] in the EU, the Irish Data Protection Commission's 2019 budget was EUR 15 million and the Luxembourg's authority EUR 5.5 million.[217] Although most European data protection authorities stressed the need for a significantly larger budget and personnel to

[211] European Commission, *supra* note 61, at 20;
[212] Satariano, *supra* note 4.
[213] Yuri Nagano, *California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court*, SAN FRANCISCO PUBLIC PRESS, May 15, 2019, https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak.
[214] Leah Nylen, *FTC suffering a cash crunch as it prepares to battle Facebook*, POLITICO (2020), https://www.politico.com/news/2020/12/10/ftc-cash-facebook-lawsuit-444468.
[215] Stigler Center, *supra* note 116, at 220.
[216] CPRA Sec. 24.18.
[217] AccessNow, *supra* note 182, at 11.

appropriately enforce their new expanded legal responsibilities "almost none of them received the requested amount [of funding]."[218]

Finalizing the stylized pub example, as a third alternative to remedy the violation the aggrieved consumer could complain to a dedicated regulator that its name and phone data had been illegally collected and processed. In this case, however, the consumer cannot enforce the law directly—first it will have to convince a public agent to open an investigation into the matter. The consumer, however, is not aware of which pub shared the data, so the agent must require the pubs in the areas to produce the information needed to enforce the law. The consumer is then only updated every three months that investigations are ongoing, but there is hardly anything it can do to accelerate the process. The same public agent, however, oversees data processing in the entire city, so it must simultaneously handle thousands of other complaints. Pubs also generally refuse to share the information the agent needs to finalize the case, as they profit from it. In addition, the pub industry is responsible for 26% of the country' exports and 10% of its employment, and many pubs settled in that specific jurisdiction because it has somewhat permissive data use laws.[219] The agent, therefore, knows that the government does not want to antagonize that industry—in fact, the agents' boss had meetings with pub owners to help understand their data needs. After years, the regulatory agency issues a fine that amounts to 0.1% of what the pub in question earned in profits in the preceding year.[220] The pub still has the option to appeal the fine before the judiciary, further delaying the enforcement of the law.

[218] European Data Protection Board, *supra* note 210, at 5.
[219] The same data for the importance of the digital economy to Ireland. See footnote 194 above.
[220] The first fine issued by the Irish DPA against a leading tech company, Twitter, took almost two years of investigation (despite being a simple, objective case of the company not complying

Again, this is a stylized example. Yet, it touches in only some of the challenges of developing an effective regulatory system for complex data collection and processing practices. Mandates are broad and large information asymmetries and market power significantly increase the public resources needed to enforce the laws and the risks of both private and public capture.

III. NARROWING DATA PROTECTION'S ENFORCEMENT GAP THROUGH INSTITUTIONAL DESIGN

Regulatory systems must be designed to anticipate implementation challenges and facilitate monitoring and enforcement. Yet, online privacy laws like the CCPA (even after the CPRA amendments) and the GDPR have been failing to fully account for how exceptionally large information asymmetries and market power usually found in many data markets undermine markets, torts and regulatory enforcement as mechanisms to ensure that companies reflect consumers' data privacy preferences. As mentioned in Part I above, it is possible that some form of compliance improves as these regimes mature. Yet, past experience shows that this improved compliance is in no way guaranteed.[221] Societies are now spending billions of scarce private and public resources in systems with important flaws. Narrowing data protection's enforcement gap will require improving the institutional design of these laws—by paying more attention to what happens in the shadows of the law, scholars and policymakers can help ensure not only that these

---

with a 72-hour data breach notification deadline) and amounted to approximately USD 550,000, or 0.1% of Twitter's 2019 profits. Natasha Lomas, *Twitter fined ~$550K over a data breach in Ireland's first major GDPR decision*, TECHCRUNCH , https://social.techcrunch.com/2020/12/15/twitter-fined-550k-over-a-data-breach-in-irelands-first-major-gdpr-decision/.

[221] As seen above, compliance with the Directive 95/46 or the European E-privacy directive has been extremely low, despite their enactment decades ago.

regimes better deliver on their promises, but that they do so in quicker and more cost-effective way.

It is beyond this paper to provide definitive solutions to the multiple and complex issues identified above. First because most of these will be jurisdiction specific, requiring changes to the different laws that regulate public transparency, standing, discovery, causation, the filing of lawsuits for failure to act, etc. (each likely demanding a paper of its own); and second because one cannot rule out that these systems may require a significant rethinking of their fundamental goals.[222] Rather, the objective here is to learn from the way in which more mature regulatory regimes such as antitrust and anti-corporate fraud have tackled the common challenge of large *information asymmetries* undermining legal compliance: if they are not addressed, it is unlikely that any privacy laws will fully deliver on their goals. This focus on information asymmetries is justified because the antitrust community is already actively discussing how to diminish the market power of large digital platforms,[223] but the equally important role of these asymmetries in undermining data protection compliance has been largely neglected.

In particular, an improved data protection regulatory system should incorporate at least three key principles: (i) multiplying available monitoring and enforcement resources; (ii) bringing violations to the attention of monitors/enforcers; and (iii) forcing governmental accountability as a way to diminish risks of regulatory capture.

[222] See Waldman, *supra* note 44, at 825, discussing other structural changes to privacy laws that would also be important to help promote compliance.
[223] See Lancieri and Sakowski, *supra* note 13, for a general review of diagnosed concerns and potential remedies.

i. Multiplying monitoring and enforcement resources

Not only the collection and processing of personal data is usually taking place in complex, non-transparent environments, but the widespread collection and easy replicability of these data expands the jurisdiction of online privacy laws. As seen above, this combination undermines monitoring and enforcement in systems that rely primarily on regulatory enforcement, like the GDPR and the CCPA.

Important information asymmetries, however, are not exclusive to data protection (even if they are exacerbated in it). Anti-corporate fraud and antitrust policies also face challenges in discovering intra-corporate wrongdoing in complex environments. To help tackle this problem, however, these regimes have been designed to encourage that sophisticated private organizations understand the complexity of corporate practices and denounce violations: for example, a large survey on corporate fraud lawsuits in the US found that regulators exposed only 20% of wrongdoing, with the remaining 80% being exposed by employees, the media/academia, industry analysts and other sophisticated third-parties;[224] and the majority of US antitrust litigation is private, not public.[225] Data protection laws should be equally designed to expand the number of sophisticated private intermediaries—such as privacy NGOs, independent think-tanks and class-action plaintiffs—that have the expertise and resources to comprehend the complexity of data processing and act alongside public regulators in detecting violations. These sophisticated civil society intermediaries

[224] Alexander Dyck, Adair Morse & Luigi Zingales, *Who blows the whistle on corporate fraud?*, 65 J. FINANCE 2213–2253 (2010), at 2225.
[225] United States, *Submission of the United States to the OECD on the Relationship Between Public and Private Antitrust Enforcement* (2015), https://www.justice.gov/atr/file/823166/download, at 3.

are also better equipped to constantly monitor regulatory action, increasing the costs of capturing regulators.

An expansion of these sophisticated private intermediaries, however, requires the availability of appropriate and independent funding. This is currently not the case, as most privacy NGOs and other similar organizations are supported by grants and donations, an unreliable and insufficient source of funding for mass oversight.[226] An effective online privacy regulatory system should ensure a consistent, independent source of funding for these intermediaries, enabling them to invest time and resources in hiring technical personnel, starting complex and potentially unfruitful investigations and/or litigation and better equipping them to resist the temptation of being co-opted by large corporate donations.[227]

There are different mechanisms to help ensure that private parties have incentives to specialize in this field. For example, the US legal system foresees treble damages for antitrust violations as a way to encourage private litigation, something that the Supreme Court has said works as "a chief tool in the antitrust enforcement scheme"[228] that encourages litigants to serve as "private attorneys

[226] For example, even the most well-known European NGOs like NYOB and La Quadrature du Net have trouble raising resources. NYOB has so far raised only 66% of its EUR 500.000 funding goal for 2020, La Quadrature's raised only 70% of its 2020 EUR 400.000 goal. See https://support.noyb.eu/funding; https://www.laquadrature.net/en/about/. In the US, the Electronic Privacy Information Center, another large NGO, had a budget of roughly USD 2 million in 2018. See https://www.epic.org/epic/EPIC-2018-Audit.pdf, at 6.

[227] A problem that exists in antitrust. See, Tony Romm, *Amazon, Facebook and Google turn to deep network of political allies to battle back antitrust probes*, WASHINGTON POST (2020), https://www.washingtonpost.com/technology/2020/06/10/amazon-facebook-google-political-allies-antitrust/; Daisuke Wakabayashi, *Big Tech Funds a Think Tank Pushing for Fewer Rules. For Big Tech.*, THE NEW YORK TIMES, July 24, 2020, https://www.nytimes.com/2020/07/24/technology/global-antitrust-institute-google-amazon-qualcomm.html.

[228] Hawaii v. Standard Oil Co., 405 U.S. 251, 262 (1972).

general".[229] This is certainly an important mechanism to be considered, even if it has limitations and is of difficult acceptance abroad.[230]

A likely more acceptable institutional design alternative that jurisdictions should consider is to create a system of recurrent grants that is linked to how well these intermediaries perform their role. These grants would be funded by the resources raised from fines and damages awards associated with data protection violations and would be distributed according to both a direct and an indirect method. Under the direct method, the laws could establish that private parties such as NGOs, data-focused investigative news agencies[231] or other intermediaries are entitled to a small percentage: (i) of the fines that result from an investigation that started from a private complaint; or (ii) of the damages awarded in tort litigation where these organizations represent consumers. Under the indirect method, a panel of public authorities and civil society representatives could annually distribute grants to NGOs, universities, think tanks, dedicated investigative news agencies and other private organizations that are engaged in projects aimed at improving data protection. This mechanism has several advantages: it can ensure long-term funding for these organizations, rather than large lump-sum awards followed by periods without any resources; it can be implemented without changes that impact the perceived justice of tort law and it directly connects funding to effective monitoring, minimizing administrative costs.

Again, antitrust policies can provide an example on how the indirect method would work. Brazilian antitrust laws establish that fines imposed by the Brazilian competition authority are allocated to a public fund aimed at protecting citizens' diffuse interests—in 2019, the fund raised

[229] Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614, 635 (1985).
[230] See, generally, Daniel A. Crane, *Optimizing private antitrust enforcement*, 63 VAND REV 673 (2010). (discussing limitations in American private antitrust enforcement).
[231] Such as https://themarkup.org, a non-profit, investigative journalism newsroom focused on investigating large tech platforms.

approximately USD 120 million.[232] This fund is managed by a council composed of seven career civil servants and three civil societies representatives, appointed for a renewable mandate of two-years.[233] The fund annually publishes public calls for applications through which universities, NGOs and even other entities can request resources to support their activities in defense of the public interest. In 2019 alone the fund awarded 46, long-term grants. Here, it is also worth mentioning the changes brought about by the CPRA, which are an important step in this direction. Section 18 of the new law foresees that nine percent of the Consumer Privacy Fund that collects CCPA damage awards (and that currently goes mostly to the Californian treasury) will be distributed by the California Privacy Protection Agency as grants to civil society and law enforcers.[234] The three percent that would go to NGOs, however, seems insufficient to bring monitoring resources to levels that can actually diminish the high levels of information asymmetries in data protection.[235] Such levels should be enlarged, and European countries should also adopt similar initiatives.

The direct funding system, on the other hand, could be an expansion of the already common US practice of directing *cy pres* awards in class action lawsuits to privacy NGOs.[236] A problem with these *cy pres* settlements in data protection is the occasional distribution of awards to organizations

[232] Article 28, §3 of Law 12.529/11 and the public information on the resources of the fund, available at https://www.justica.gov.br/seus-direitos/consumidor/direitos-difusos/arrecadacao-1
[233] Article 3 of Brazilian Presidential Decree 1.306/94.
[234] Section 18 of the CPRA. The distribution would be: (i) 3% to nonprofit organizations to promote and protect consumer privacy; (ii) 3% to nonprofit organizations and public agencies to educate children in the area of online privacy; and (iii) 3% to state and local law enforcement agencies to fund cooperative programs with international law enforcement organizations.
[235] Even if CCPA fines reach unprecedented USD 100 million, this would lead to an annual distribution of USD 3 million dollars, not enough to support many large-scale organizations with lawyers, tech specialists, etc.
[236] COMMITTEE ON DIGITAL PLATFORMS FINAL REPORT, STIGLER CTR. FOR THE STUDY OF THE ECON. AND THE STATE AT CHICAGO BOOTH 23 (2019), https://perma.cc/RWV9-KRL5, at 220.

that are not directly connected to online privacy.[237] To address this, the law could encourage that awards are funneled to the public fund, which would then ensure that *cy pres* resources are distributed more broadly and fairly.

Both proposals have limitations of their own. First, they focus on deterrence rather than victim compensation—a choice justified at a moment when enforcement levels are low, but this could change in the future. Privacy class actions settlements could also continue to be unduly funneled to plaintiffs' lawyers and/or to organizations that do not protect consumer privacy[238] and/or that a public grant system can be diverted to accomplish interests other than what it was initially envisioned.[239] To prevent this, it would be important that judges closely monitor settlements and that laws create a centralized, public database that lists all damages awards and public grants to enable oversight. Laws may also foresee that the fund has an obligation to award at least a percentage of its annual budget, impose strict conflict of interest rules and increase the number of independent civil society representatives that are part of the management council. Finally, different jurisdictions should set different funds, ensuring some form of competition over governance.

Still, a data protection regulatory regime that expands the funding of independent and sophisticated data privacy intermediaries—allowing them to tap on donations, grants and/or awards from tort litigation—would be much more capable of detecting wrongdoing than one overtly reliant on public regulators.

---

[237] Rotenberg and Jacobs, *supra* note 128, at 309, 321, quoting Marek v. Lane, 134 S. Ct. 8, 8–9 (2013).
[238] *Id.* at 309.
[239] The Brazilian fund did not award grants for many years as the government earmarked the funds to help diminish the public budget deficit.

ii. Bringing data protection violations to light

The information asymmetries between how companies collect and process personal data and what civil society and regulators know about it increase the importance of mechanisms designed to bring violations to the attention of these overseers. A stronger, better-funded civil society will increase monitoring resources. Yet, another comparison with antitrust, anti-corruption/anti-corporate fraud regimes showcases the importance of the regulatory system also encouraging insiders to report illegal behavior through the establishment of a solid whistleblowing program.

Whistleblowers (in particular employees) are key to the discovery of corporate fraud.[240] Antitrust regulators have also long relied on leniency programs—through which companies denounce cartels in exchange for a more lenient prosecution—as a key mechanisms to bring otherwise secret and illegal private deals to light. Indeed, past studies have found that having access to privileged, internal information greatly increases the probability of successfully exposing hidden fraud.[241]

[240] Dyck, Morse and Zingales, *supra* note 224, at 2225 (surveying 216 high-profile corporate fraud cases in the US and finding employees, non-financial markets regulators, business analysts and the media (sophisticated third parties) responded for 54% of all corporate frauds exposed, with employees being the most important at 17% of cases). Andrew C. Call et al., *Whistleblowers and outcomes of financial misrepresentation enforcement actions*, 56 J. ACCOUNT. RES. 123–171 (2018) at 128 (reviewing 658 SEC enforcement actions for fraud and finding that "employee whistleblowing plays an integral role in monitoring firm behavior"); OECD, *Detection of Foreign Bribery: The role of Whistleblowers and Whistleblower protection* (2017), http://www.oecd.org/corruption/anti-bribery/OECD-The-Role-of-Whistleblowers-in-the-Detection-of-Foreign-Bribery.pdf. at 3, 11 (stressing the key role whistleblowers play in revealing wrongdoing).

[241] Dyck, Morse, and Zingales, *supra* note 224, at 2215, 2230-31. (Finding that a potential detector without access to internal company data is 15% less likely to blow the whistle). Call et al., *supra* note 240, at 126 (finding that whistleblowers are associated with larger monetary penalties for targeted firms and larger prison sentences for employees).

Financial incentives associated with the revealing of the fraud also significantly improve the probability of employees exposing wrongdoing and diminish wrong denunciations.[242]

Increasing compliance with online privacy laws will require redesigning regulatory systems to bring otherwise obscure violations to light. These comparative experiences showcase the importance of data protection authorities establishing solid whistleblowing programs specifically aimed at encouraging the reporting of data protection violations.[243] In particular, it is key that this program:

i. Defines a "whistleblower" broadly to include not only formal employees but also contractors, consultants, former employees, temporary employees, etc.[244] The program should also protect public employees who may report potential capture of regulatory authorities;

[242] Dyck, Morse, and Zingales, *supra* note 224, at 2246-47, (finding that whistleblower employees with financial rewards responded for 41% of frauds exposed in the healthcare industry, where there are financial incentives to report cases, versus 14% in other industries without such incentives. Also finding that frivolous corporate fraud lawsuits are lower in the healthcare than in other industries. A potential detector with financial incentives is 27% more likely to reveal significant fraud). OECD, *supra* note 240, at 11.

[243] Both the California and the EU have general whistleblowing protections: in California, the California Whistleblower Protection Act, the False Claims Act and California Labor Code Section 1102.5 provide general protections against retaliation for revealing wrongdoing; in the EU, Directive 2019/1937 from October 2019 establishes minimum levels of whistleblowing protection around the Union and states that these laws should include, among many others areas, violations of data protection laws (Article 1(a)(x)). Yet, the translation of these commands to a dedicated data protection program is lagging, to say the least. At the moment of this writing, California has no dedicated data protection whistleblowing program, nor have important EU jurisdictions such as Ireland or Luxembourg. These general provisions also fall short of many recommendations made herein. For example, the EU Directive does not encourage financial rewards that are key for an effective program. See Dimitrios Kafteranis, *Rethinking Financial Rewards for Whistle-Blowers Under the Proposal for a Directive on the Protection of Whistle-blowers Reporting Breaches of EU Law*, 2 NORD. J. EUR. LAW 38–49 (2019).

[244] OECD, *supra* note 240, at 15.

ii. Raises awareness of the protections afforded by the program to potential reporting persons by hosting workshops, requiring corporate training and publicizing the program broadly in specialized channels and in the media;[245]

iii. Allows for potential whistleblowers to obtain confidential advice from the public authority before filing a report. This has been done, for example, both in The Netherlands and in the US, where the SEC created a dedicated, specialized whistleblower hotline to provide guidance to potential corporate-fraud whistleblowers.[246] As an alternative, the data protection fund discussed above could provide resources to independent, private third-parties like NGOs dedicated to protecting and guiding potential whistleblowers or even representing them before authorities;[247]

iv. Protects the anonymity of whistleblowers.[248] For example, in Austria, corporate-fraud whistleblowers are allowed to create a unique, secure and official mailbox with pseudonym and password to protect their confidentiality while exchanging information.[249] This also allows the authority to provide feedback to the whistleblower and keep it updated about the status of the claim;

v. Provides financial rewards for successful reports. Financial rewards are key to encourage whistleblowing, as employees risk ending their careers for revealing the wrongdoing.[250]

---

[245] *Id.* at 4.
[246] *Id.* at 7-8.
[247] *Id.* at 9.
[248] Dyck, Morse, and Zingales, *supra* note 224, at 2240, 2245, (finding that in 37% of cases employee whistleblowers do not identify themselves and that in 82% of cases where employees were named, the individuals were fired, quit under distress or had significantly altered responsibilities as a result of revealing the wrongdoing).
[249] OECD, *supra* note 240, at 10.
[250] Dyck, Morse, and Zingales, *supra* note 224, at 2251 ("a natural implication of our findings is that the role of monetary incentives should be expanded").

These rewards should be large enough to encourage whistleblowing and also should have minimum thresholds, to help prevent frivolous claims. For example, In the US, SEC awards range between 10-30% of the money collected as a result of the whistleblower denunciation, as long as the sanctions are above USD 1 million;[251]

vi. Protects good-faith whistleblowers from retaliation, including broad civil remedies or even punitive damages for whistleblowers that have been retaliated against.[252] Most whistleblowers first report wrongdoing internally to the company, only resorting to regulators whenever companies refuse to take action.[253] The law should make clear that these employees are equally protected and can require that companies have an obligation to forward any serious whistleblower complaints to regulators within a given period. It should also shield good faith whistleblowers when they report wrongdoing to journalists and other private intermediaries that can raise awareness to potential problems; and

vii. Protects whistleblowers from legal/criminal charges regarding slander, violation of trade secrets, corporate espionage and even civil defamation lawsuits that can be used by well-resourced organizations to silence reporting parties.[254]

All of these principles must be adapted to the laws of specific jurisdictions. Nonetheless, a dedicated data protection whistleblower program that incorporates most of these principles would help diminish information asymmetries and increase the enforcement of online privacy.

[251] OECD, *supra* note 240, at 11.
[252] *Id.* at 19.
[253] *Id.* at 14.
[254] *Id.* at 11.

iii. Increasing governmental accountability

Finally, while some characteristics of data protection weaken exit and voice and reinforce the importance of a solid public enforcement system, data policy's heightened risk of capture by private or public interests also reinforces the need for institutional safeguards to protect the public interest. Many important data protection agencies such as the those of Ireland, Luxembourg and even the FTC are unjustifiably opaque. By requiring authorities to publicize a wide-range of information about their enforcement actions, online data privacy regimes can diminish the costs of private oversight and help expose eventual problems—sunshine is the best of disinfectants when fighting entrenched private interests.

Again, a comparison with antitrust laws can help showcase a way to improve the design of data protection laws. For example, extensive public disclosure rules have been instrumental in helping understand the role of corporate donations in influencing policy advice in competition policy[255] and multiple reports have suggested enhancing transparency obligations for US antitrust authorities as a way to increase public confidence in regulators and hinder attempts of regulatory capture.[256] Extensive discovery rights have also helped expose many cases of corporate malpractice.[257]

[255] See Wakabayashi, *supra* note 227.
[256] THE FED. TRADE COMM'N AT 100 REPORT—INTO OUR 2ND CENTURY: THE CONTINUING PURSUIT OF BETTER PRACTICES (Jan. 2009) at 119–20; THE NEXT ANTITRUST AGENDA: THE AMERICAN ANTITRUST INSTITUTE'S TRANSITION REPORT ON COMPETITION POLICY TO THE 44TH PRESIDENT OF THE US (2008) at 187; ANTITRUST MODERNIZATION COMMISSION, REPORT AND RECOMMENDATIONS (2007) at 64-65.
[257] Roy Shapira & Luigi Zingales, *Is pollution value-maximizing? The DuPont case*, NBER WORK. PAP. 23866 (2017), at 8 (showcasing how internal DuPont documents exposed at trial where key to discovery of illegal practices by the company).

Some antitrust systems have been expressively designed to maximize transparency as a way to help fight regulatory capture without undermining enforcement capacity. The Brazilian experience is noteworthy. Brazil's competition law establishes that antitrust proceedings should be public by default, but that the private parties may request or the regulator may determine that certain types of information are confidential.[258] To comply with this legal requirement, CADE (the Brazilian antitrust authority) created a system where private parties are required to prepare both a public and a confidential version of any document they file before CADE. CADE's systems also host public and confidential versions of all of CADE's opinions—including statements of objections or opinions to approve a merger or dismiss an investigation. All the public version of both private and public documents are freely available on CADE's website, while the private versions are protected by secrecy laws. Some investigations require absolute secrecy (e.g. cartel investigations before dawn raids). For those, CADE maintains a smaller public and a more extensive private record but both are confidential until the authority rules that publicity will not harm the investigation nor the parties involved. However, ultimately the public record is made available to civil society.

Requiring private parties to disclose in advance what specific pieces of information they understand as confidential is important because it: (i) expedites disclosure; (ii) allows CADE to focus potential disputes in some key central pieces of data over which there is disagreement; and (iii) allows interested private parties to better understand and challenge abusive confidentiality requests. While this system increases administrative costs, this structure that requires private parties to cooperate in implementing regulatory transparency helps minimize negative impacts on enforcement actions. Indeed, CADE hosts one of the most active anti-cartel programs in the world

[258] Article 49 of Brazilian Law 12.529/11.

and—despite Brazil's history of corruption—CADE's work is well-recognized by Brazilians and international organizations.[259]

Data protection laws should impose similar obligations on regulators. In particular, it would be important that regulators: (i) maintain a webpage that lists ongoing investigations, describing the scope of the investigation and the interested parties; (ii) upload to this webpage public versions of new case developments such as statements of scope and indictments (e.g. Statements of Objection) as well as company's responses; and (iii) upload to this webpage public version of opinions/settlements as well as at least a short but precise justification on the reasons why authorities decided to close investigations, settle cases or impose fines.

IV. CONCLUSION

The GDPR, the CCPA, the CPRA and their dozens of international counterparts bring about profound changes: data markets, usually left almost to their own devices, now face a new environment where the state mediates at least part of the interactions between companies and consumers. Yet, data protection laws have been failing to fully deliver on their promises. This article indicates that this has been in part because legislators have not anticipated how the particularly pervasive information asymmetries and market power found in many data markets

[259] The OECD affirmed that CADE is "well regarded domestically and internationally within the practitioner community, with peer agencies and within the Brazilian administration" and praised CADE's work in prosecuting cartels. OECD, *Peer Reviews of Competition Law and Policy: Brazil* (2019), http://www.oecd.org/daf/competition/oecd-peer-reviews-of-competition-law-and-policy-brazil-ENG-web.pdf, at 9-11. In addition, the prestigious British magazine Global Competition Review considered CADE the best antitrust agency in the Americas in three of the past five years, beating international peers such as the FTC and the DoJ. CADE, *Cade is awarded the Agency of the Year in the Americas* (2018), http://www.cade.gov.br/cade_english/cade-is-awarded-the-agency-of-the-year-in-the-americas.

undermine the role of markets, torts and regulatory enforcement as mechanisms to ensure legal compliance.

Democratic governments around the world have decided that these data protection regulatory regimes are here to stay. Societies must now ensure that these laws lead to meaningful improvements on the ground. This article indicates that narrowing data protection's enforcement gap is not impossible, but it will require better institutional design. Multiplying monitoring and enforcement resources, encouraging that insiders bring violations to light and promoting regulatory accountability are important but initial solutions to help tackle a multi-faceted, complex problem. This is a field that will welcome contributions from lawyers, data and political scientists, economists, psychologists and many other scholars for years to come.

APPENDIX: SURVEY OF THE EMPIRICAL EVIDENCE ON THE GDPR'S AND THE CCPA'S IMPACT ON THE GROUND

A survey of empirical studies assessing the impacts of the GDPR and the CCPA on actual data collection and processing points to underwhelming results so far. None of the twenty-two independent studies, found meaningful compliance on the ground. In particular, fourteen studies found widespread violations.[260]

i. A review of 2,000 high profile websites found that while the GDPR did give users more privacy controls, "tracking is prevalent, happens mostly without user's consent, and opt-out is difficult". 92% of websites start tracking users before providing them with any notice and 85% continue tracking them or add even more cookies after the users opt-out;[261]

ii. A review of the privacy policies of 194 firms before and after the passage of the GDPR finds that while the vast majority amended their policies to become more information protective, "the overall level of compliance [with GDPR provisions] is not high in absolute terms";[262]

---

[260] It is worth noting that many European studies focus on the collection and processing of data through cookies, something that has limitations (as indicated below). Cookies are mostly regulated by the ePrivacy directive. However, Article 7 of the GDPR has reframed what characterizes as effective consent for the collection of personal data, including through cookies. Therefore, these studies find violations of both the ePrivacy directive and of the GDPR. This is backed by European case law, such as the European Court of Justice landmark ruling in case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH, Judgement of the Grand Chamber, ECLI:EU:C:2019:801. See Cristiana Santos, Nataliia Bielova & Célestin Matte, *Are cookie banners indeed compliant with the law? deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners*, ARXIV PREPR. ARXIV191207144 (2019). at 1-2.

[261] Sanchez-Rola et al. *supra* note 7, at 341, 344-345. Importantly, this study included both first and third party tracking.

[262] Davis and Marotta-Wurgler, *supra* note 132, at 667, 699.

iii. A study tracking 1250 top-visited European and US websites before and after the GDPR (February to September 2018) finds only a small decrease in advertising third-party requests, which the authors say they cannot directly link to the GDPR;[263]

iv. a survey of the five most popular Consent Management Platforms (CMPs) used by the UK's 10.000 most accessed websites found that by September 2019 only 11.8% of the UK websites met minimum notice and consent requirements required by law;[264]

v. a study of 1000 randomly selected EU consent notices collected by October 2018 found that 57% of these notices nudge users towards privacy-unfriendly options and 96% of them provide either no consent choice or confirmation only, violating the GDPR;[265]

vi. another study of 1426 consent banners used by Europe's 22.949 most accessed websites found that, by September 2019, 10% of websites placed cookies before giving the user any choice and 5% still placed the cookies after the user refused to give consent. All in all, the study found that 54% of websites surveyed violated legal requirements;[266]

vii. a study of cookie placements in 35.000 popular EU websites after four years of the coming into force of the European e-privacy directive found that between 49% to 74% placed tracking cookies before receiving consent (depending on definition of tracking), a percentage that stayed constant after the entry into force of the GDPR—indicating that both

[263] Jannick Sørensen & Sokol Kosta, *Before and after GDPR: The changes in third party presence at public and private european websites*, *in* THE WORLD WIDE WEB CONFERENCE 1590–1600 (2019), at 1599.
[264] Midas Nouwens et al., *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, ARXIV PREPR. ARXIV200102479 (2020), at 6.
[265] Utz et al., *supra* note 88, at 974.
[266] Célestin Matte, Nataliia Bielova & Cristiana Santos, *Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*, ARXIV PREPR. ARXIV191109964 (2019), at 2.

policies were ineffective. It points to a lack of auditing by regulators as a reason behind its failure;[267]

viii. a study analyzing the 500 most visited websites for each EU country found that, even after the GDPR (October 2018), 15% of these websites had no privacy policy, 37% of websites did not comply with cookies consent notice and the amount of consumer tracking pre- and post-GDPR mostly remained the same. The study warned against a false sense of GDPR compliance;[268]

ix. Another study of the 27.000 most accessed websites in the EU, the US and Canada found that the coming into force of the GDPR led to a 14.9% drop in the use of third-party vendors, but that this number rebounded to pre-GDPR levels by the end of 2018, potentially because firms became less afraid of enforcement actions;[269]

x. A cookie sweep of 38 large data processors by the Irish Data protection authority found that more than 18 months after the GDPR had come into force, 92% did not comply with the law;[270]

xi. An in-depth study with data covering data from 1 January 2018 to 31 July 2018 from one of the largest online travel agencies and travel meta-search engines find that the GDPR resulted in a reduction of 12.5% in total cookies (not consumers, as one consumer can have many cookies), which is a proxy for decreased online tracking. However, the remaining consumers are more persistently trackable after the GDPR, so the overall level of online tracking increases by 8%, something that should lead to increased ability to predict

[267] Trevisan et al., *supra* note 46 at 127, 133, 140.
[268] Degeling et al., *supra* note 54, at 7-8, 10, 14.
[269] Johnson, Shriver and Goldberg, *supra* note 170, at 14-15.
[270] Irish Data Protection Commission, *supra* note 8, at 6.

consumer behavior;[271]

xii. In interesting 2020 analysis of data interconnection agreements and interconnection points Internet Service Providers (a proxy for data transfers) pre and post GDPR. Contrary to expectations, they find a precise zero GDPR effect, meaning that the GDPR has not let to decreases in data traffic that could potentially impact investments in internet networks;[272]

xiii. A 2020 large scale survey of 17,000 websites and more than 7,500 cookie banners in the UK and Greece (14,000 in the UK and 3,000 in Greece) found that only 50% of websites display a cookie notice, and that the majority of websites employed dark patterns to nudge users towards acceptance. Their conclusion is that a "substantial proportion of the websites do not comply with the law [GDPR] even at the very basic level";[273]

xiv. A detailed survey of GDPR and the ePrivacy Directive requirements for consent involving the collection of information through cookies concluded that fully automatic consent verification by technical means is not compliant with both laws, yet, this is the widespread method of adoption in the EU;[274]

xv. A following study conduct in January 202 analyzed the basis for the collection and processing of personal data by more than 600 European advertisers. The findings "demonstrate the persistence of the advertising industry in non- compliant (with GDPR

---

[271] Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR*, NBER WORK. PAP. (2020), https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-guy_aridor.pdf, at 3-4, 15-18.
[272] Ran Zhuo et al., *The Impact of the General Data Protection Regulation on Internet Interconnection*, NBER WORK. PAP. 26481 (2020), https://www.nber.org/system/files/working_papers/w26481/revisions/w26481.rev0.pdf at 4, 38.
[273] Georgios Kampanos & Siamak F. Shahandashti, *Accept All: The Landscape of Cookie Banners in Greece and the UK*, ARXIV PREPR. ARXIV210405750 (2021). at 1, 14.
[274] Santos, Bielova, and Matte, *supra* note 265. at 3, 74.

and ePrivacy Directive) methods for tracking and pro- filing, bundled in often complex and vague presentation of purposes";[275]

xvi. A PwC surveyed the websites of the US' 600 largest companies done in February 2020 found that a majority of these websites did not offer portals for users to access their information;[276]

xvii. A survey by Data Grail, a US privacy management tool, found that throughout 2020 business-to-consumer companies received, on average, 137 data subject requests per million identities they hold per year, with the average stabilizing at around 11 requests per month. This means that only 0.001% of consumers are exercising their rights. That is despite average cost of almost USD 200,000 per request;[277]

xviii. While not specifically targeted at the CCPA or the GDPR, a September 2020 scan of more than 80.000 of the world's most popular websites by US-based investigative journalism website The Markup found that tracking remains ubiquitous around the world and in the US, even in highly sensitive websites such as those of abortion providers or for victims of sexual violence.278 Its general conclusions are that third-party tracking is as pervasive now as it was 10 years ago, but it has only "become creepier and more difficult to stop".[279]

[275] Célestin Matte, Cristiana Santos & Nataliia Bielova, *Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?*, *in* ANNUAL PRIVACY FORUM 163–185 (2020). at 2.
[276] PricewaterhouseCoopers, *supra* note 12.
[277] Data Grail, *supra* note 14. at 4.
[278] The Markup, *supra* note 58.
[279] The Markup, *supra* note 59.

Four studies present a more favorable picture of the GDPR's impact on the ground. Even those, however, also show only a limited impact and introduce important caveats about the state of GDPR enforcement.

xix. One study analyzed web tracking by 5100 of the most visited EU websites between September 2017 to April 2019 and finds that the GDPR was correlated with a reduction of 9% in the number of 3rd party tracking cookies for the median website and a 17% reduction in 3rd party HTTP requests. However, it also finds that the GDPR led to no change in tracking by the most pervasive companies, such as Google, Facebook, Amazon and others—these companies would have even expanded to more websites;[280]

xx. One study of 110.000 websites between May 2017 and November 2018 estimated that GDPR has led to a 12% decrease in third-party tracking cookies and a (smaller) increase in first-party cookies—what the authors see as evidence that the GDPR may have achieved some data minimization goals. The authors, however, find that 3rd party requests, which can also be seen as a proxy for tracking, rebounded to pre-GDPR levels as companies learnt how to navigate compliance. All in all, the study finds that the GDPR's impacts are potentially more pronounced in antitrust/market concentration than in privacy;[281]

xxi. A rare study comparing permissions for data access in the 50 most downloaded apps of the Android Play Story between March 2017 to December 2018 found a general decrease in the number of permission requests for apps, in particular to access contacts, location and microphone. It also found less use of these permissions in idle mode. However, it noted that apps are more frequently using permissions for camera, microphone and body sensors.

[280] Solomos et al., *supra* note 170, at 3, 6, 8.
[281] Peukert et al., *supra* note 170, at 21, 24.

The overall conclusion is that app privacy has only moderately improved since the GDPR's entry into force;[282] and

xxii. Finally, one study using Adobe Analytics data for 1084 dashboards finds that the GDPR led to a decrease of 11.7% in page views for European websites and a 13.3% revenue fall for e-commerce websites. This would be partially motivated (6.9-29%) by users do not providing consent to data collection and by decreases in paid marketing channels as drivers of traffic. While the study does not assess data collection nor impacts on web-tracking, it states both that the vast majority of websites in their sample adopts an opt-out approach for consent, which is in violation of data protection laws and that changes in marketing budgets are consistent with some websites moving ads from channels that rely on personal data to others that do not. Overall, the study find "modest progress" towards GDPR compliance.[283]

Importantly, although very valuable, these studies have a selection bias in reporting what they can count readily—they usually use third-party cookies as proxies for tracking because this is what can be measured by external sweeps. This methodology, however, has important limitations:

First, these sweeps cannot measure how much data is actually collected through each cookie, so they are an imperfect proxy at best.

Second, many companies (such as Google and Facebook) responded to data protection laws not by diminishing data collection but rather by embedding their third-party code in first-party

[282] Nurul Momen, Majid Hatamian & Lothar Fritsch, *Did App privacy improve after the GDPR?*, 17 IEEE SECUR. PRIV. 10–20 (2019), at 16-17, 19.
[283] Samuel Goldberg, Garrett Johnson & Scott Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR*, (2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421731, at 2-3, 18, 26, 34, 38.

applications.[284] There are even fewer studies addressing legal compliance with regards to equally intrusive but less "transparent" tracking mechanisms such as pixels, tags, fingerprinting, localStorage, browser extensions, single sign-on or even direct matching and sharing of personal data. A large survey on browser fingerprinting, for example, argued that their increasing prevalence and stealth nature made it "particularly dangerous" to the privacy of users.[285]

Third, many cookie sweeps also restrict their analysis to homepages, but studies found more pervasive online tracking beyond the homepage.[286]

Fourth, there are few studies looking on how these laws have impacted tracking outside of the browser world, in particular in mobile/mobile apps and smart devices. That is despite the fact that mobile apps have been found to be more invasive than browsers, and other evidence points to widespread collection of personal data by mobile apps and devices.[287]

When considering those, it is likely that online privacy violations are much more widespread than what has been diagnosed.

[284] Competition and Markets Authority, *supra* note 76, app. G, at 107-8 (explaining the shift and how it enables continued tracking despite decreases in third-party cookies).
[285] Pierre Laperdrix et al., *Browser fingerprinting: A survey*, 14 ACM TRANS. WEB TWEB 1–33 (2020). at 26.
[286] For example, Englehardt and Narayanan, *supra* note 81, at 18, reported an average of 20 trackers per website homepage. When they visited 4 pages within websites for a small subsample, the average number of trackers increased to 34 per page.
[287] Papadopoulos et al., *supra* note 82, at 154, 158; Competition and Markets Authority, *supra* note 76, app. G, at 37.