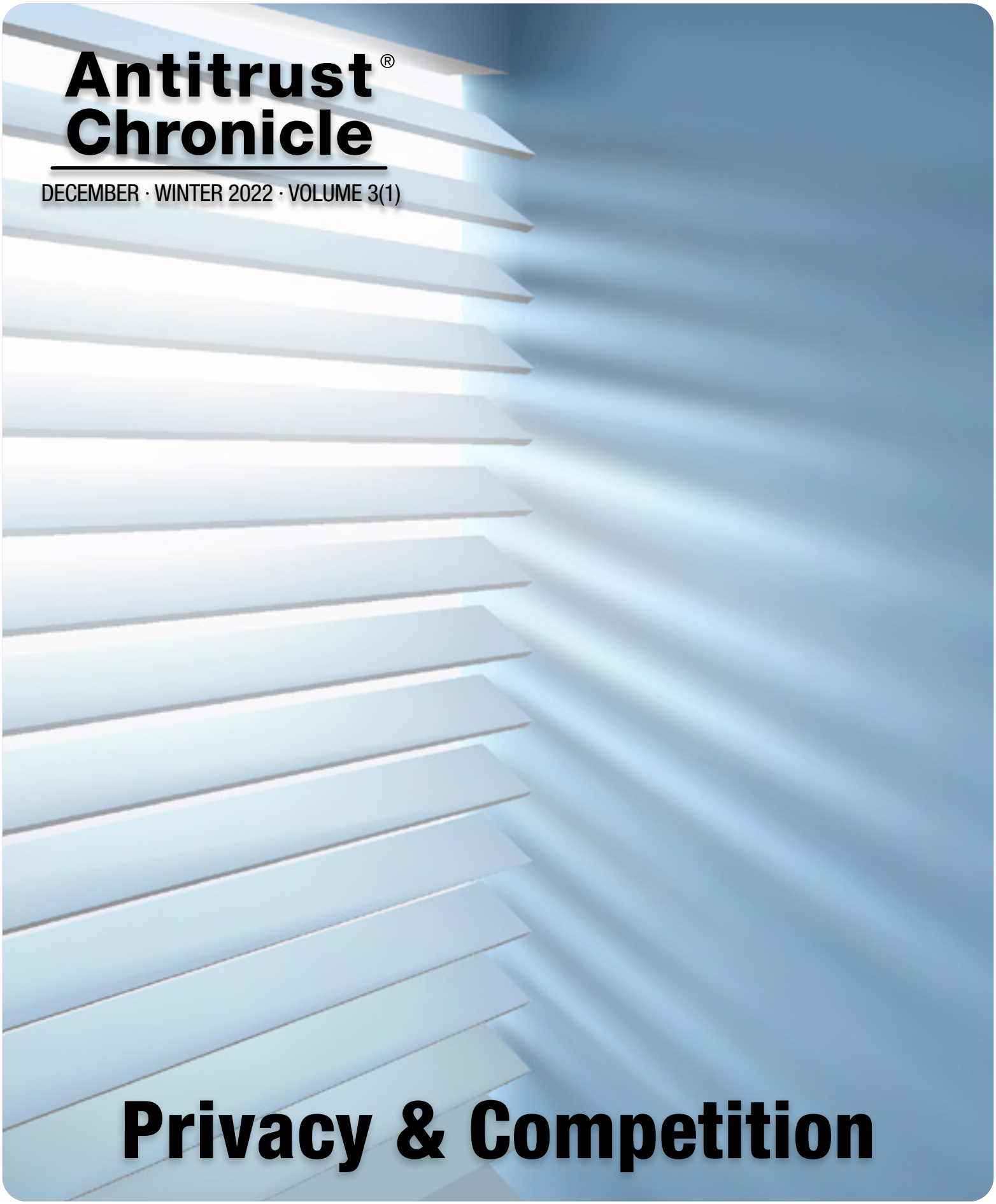
Antitrust® Chronicle

DECEMBER · WINTER 2022 · VOLUME 3(1)



Privacy & Competition

CPI COMPETITION POLICY® INTERNATIONAL

TABLE OF CONTENTS

LETTER FROM THE EDITOR

Dear Readers,

As consumers worldwide increasingly entrust online platforms with their sensitive user data, regulation (both in terms of specific privacy or data protection rules, and antitrust rules) have scrambled to keep pace. Data has famously been called the "oil" of the new economy. Just like oil, raw data is not valuable in and of itself. Rather, its value is created when it is collated quickly, completely, and accurately, and connected to other, similarly relevant data. How such data is used and shared between companies is therefore key to its value, and this raises obvious privacy (and competition) problems.

As a result, the so-called "data economy," which is the basis for many digital products and services, has been recently facing pressure from a number of regulations worldwide that aim to protect user privacy.

Individual companies, too, have adopted policies that claim to protect user privacy on their platforms. **Reinhold Kesler** opens with a discussion of Apple's App Tracking Transparency ("ATT") rules as a representative example of such a policy. Following a brief description of ATT, the author reviews the current state of research and investigations by competition authorities to provide insights on the possible effects of the privacy change.

Building on this, **D. Daniel Sokol & Feng Zhu** further expound on Apple's ATT policy. In a prior piece, the same authors claimed that this policy in fact masked anti-competitive conduct that would have been identified under traditional antitrust theories. Further, they suggested that the policy could potentially have the effects of enhancing the dominance of iOS among mobile operating systems, and the dominance of Apple's own apps and services within the iOS ecosystem. This, they claimed, would have the effect of reducing consumer choice and undermining the "free" app ecosystem enabled by personalized advertising. In this updated piece, they reexamine the issue in light of a year's worth of data since the introduction of the policy. Their contention in this new piece is that the overall empirical record supports the conclusions that: (1) competition and privacy can be at odds; and (2) that Apple's ATT policy has made app developers, particularly small and new firms, worse off.

In a novel article, **Alex Marthews & Catherine Tucker** discusses how, following on from the Snowden revelations regarding mass surveillance by the U.S. government, it is now known that chilling effects from government surveillance and other privacy violations exist. Further, these effects can at least sometimes be quantified, and significant proportions of citizens in many countries describe themselves as being harmed by them, and alter their behavior in response. What is less well established is how a government's interest in maintaining mass surveillance programs could affect competition. This article studies this question.

Ginger Zhe Jin, Ziqiao Liu & Liad Wagman discuss how COVID-19 changed work and leisure, including leading people to spend more time using mobile apps. The authors present findings from a large database of mobile apps, and discuss how pandemic-amplified demand reshaped app entry and market competition among popular apps. Interestingly, the authors note that relative to five of the largest EU economies, the U.S. has seen more breakthrough new apps after the onset of the pandemic.

Taking a U.S. perspective, **Daniel A. Hanley & Karina Montoya** comment on how antitrust enforcement can operate as a supplement to privacy protections, by providing consumers with robust privacy protections, despite the lack of a comprehensive U.S. federal privacy law. The authors argue that antitrust enforcement can be used to provide consumers baseline privacy protections by creating a market for privacy protections, targeting specific conduct such as mergers, monopolization, and deception, and imposing broad structural remedies inhibiting and deterring certain conduct.

Giuliana Galbiati & Henri Piffaut further discuss the evolving interactions between privacy and competition rules. While some initially argued that privacy was a distinct and complex issue and that competition enforcement should stay in its own lane, market realities and digitization have since then forced regulators to reflect upon how the two policies are interrelated and increase their coordination efforts. Regulations like the EU GDPR attempt to give substance to privacy rights through defining mandated levels of protection and consent. With the ensuing decrease in the asymmetry between platforms and users, privacy protection can become a relevant competition parameter. The question is then how to best inform competition policy of privacy issues.

Finally, **Victor Oliveira Fernandes** notes a crucial area of complementarity between competition and data protection law regimes. This is by ensuring greater data mobility through data portability, interoperability, and open data standards in digital markets. The paper discusses how antitrust agencies would evaluate dominant platforms' strategies to prevent data interoperability as an abuse of dominance violation against the backdrop of Brazilian experiences.

No matter what the jurisdiction, however, the critical choices to be made by antitrust and privacy authorities involve defining the limits of intervention regarding the design of digital products. The articles in this volume address the relevant questions from a number of perspectives. Each brings valuable insight to this evolving and increasingly topical area of debate.

As always, many thanks to our great panel of authors.

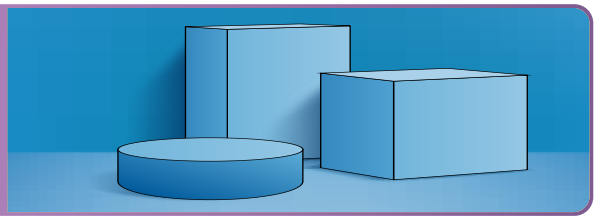
Sincerely,

CPI Team[1]

1 CPI thanks Meta for their sponsorship of this issue of the Antitrust Chronicle. Sponsoring an issue of the Chronicle entails the suggestion of a specific topic or theme for discussion in a given publication. CPI determines whether the suggestion merits a dedicated conversation, as is the case with the current issue of the Chronicle. As always, CPI takes steps to ensure that the viewpoints relevant to a balanced debate are invited to participate and that the quality of our content maintains our high standards.

SUMMARIES

8



DIGITAL PLATFORMS IMPLEMENT PRIVACY-CENTRIC POLICIES: WHAT DOES IT MEAN FOR COMPETITION?

By Reinhold Kesler

The data economy, which is the basis for many digital products and services, has been recently facing headwinds by a number of regulations worldwide that aim to better protect user privacy. Notably, digital platforms now increasingly often announce and implement privacy-centric policies. In this article, Apple's App Tracking Transparency ("ATT") is studied as a representative example of such. Following a brief description of the policy, the remainder of the article primarily reviews the current state of research and investigations by competition authorities to provide insights on the possible effects of the privacy change. While the focus is on the implications the policy has for competition in Apple's mobile ecosystem, the article also highlights the platform's role in deciding potential winners – including themselves – with its implementation of the policy and discusses weighing the potential costs against the benefits through improved user privacy.

13

HARMING COMPETITION AND CONSUMERS UNDER THE GUISE OF PROTECTING PRIVACY: REVIEW OF EMPIRICAL EVIDENCE

By D. Daniel Sokol & Feng Zhu

Apple proposed the new "App Tracking Transparency" ("ATT") policy in November 2020 and required all apps to have this feature enabled on April 26, 2021, which was the beta release of iOS 14.5. The policy prohibits apps from engaging in any activity that Apple defines as "tracking" unless the apps prompt users for "permission to track [them] across apps and websites owned by other companies" and users explicitly opt in to "tracking." In a prior essay, we identified that this policy actually masked anti-competitive conduct under traditional antitrust theories. Further, we suggested that the policy would have the pernicious effects of enhancing the dominance of iOS among mobile-operating systems ("OSs") and the dominance of its own apps and services within the iOS ecosystem, while reducing consumer choice and devastating the free-app ecosystem enabled by personalized advertising. In this essay we reexamine the issue with the benefit of a year of data. The overall empirical record on competition and privacy scholarship as well as ATT specific scholarship lead to the conclusions that: (1) competition and privacy can be at odds; and (2) that Apple's ATT policy has made app developers, particularly small and new firms, worse off. The ATT policy has done so by masking anti-competitive conduct under the guise of privacy protection.

20

EFFECTS OF GOVERNMENT SURVEILLANCE ON COMPETITION

By Alex Marthews & Catherine Tucker

Following on from the shock of the Snowden revelations, it is now well established empirically that chilling effects from government surveillance and other privacy violations exist, that they can at least sometimes be quantified, and that significant proportions of citizens in many countries both describe themselves as being harmed by them, and alter their actual behavior in response. What is less well established or understood is how a government's interest in maintaining mass surveillance programs could affect competition. This article studies this question.

25

POPULAR MOBILE APPS IN THE PANDEMIC ERA: A GLIMPSE AT PRIVACY AND COMPETITION

By Ginger Zhe Jin, Ziqiao Liu & Liad Wagman

COVID-19 changed work and leisure, including more time spent on mobile apps. While this presents an opportunity for new apps to compete with established apps, it is also challenging for new apps to grow and survive, given potentially heightened privacy concerns and ongoing government efforts to tackle data issues. We present descriptive findings from a large database of mobile apps, and discuss how pandemic-amplified demand reshaped app entry and market competition among popular apps. We find that relative to five of the largest EU economies, the U.S. has seen more breakthrough new apps after the onset of the pandemic.

SUMMARIES

35

PRIVACY PROTECTIONS THROUGH ANTITRUST ENFORCEMENT

By Daniel A. Hanley & Karina Montoya

Daniel A. Hanley & Karina Montoya comment on how antitrust enforcement can operate as a vital supplement providing consumers with robust privacy protections, despite the lack of a comprehensive federal law. The authors argue that antitrust enforcement can be used to provide consumers baseline privacy protections by (1) creating a market for privacy protections, (2) targeting specific conduct such as mergers, monopolization, and deception, and (3) courts imposing broad structural remedies inhibiting and deterring future violative conduct.

42

HOW CAN COMPETITION POLICY AND PRIVACY PROTECTION POLICY INTERACT?

By Giuliana Galbiati & Henri Piffaut

While some initially argued that privacy was distinct and independent from competition enforcement, market realities and digitization have since then forced regulators to reflect upon how the two policies can be interrelated and increase their coordination efforts. Regulations like GDPR have rebalanced the asymmetry between platforms and users enabling privacy protection to become a relevant competition parameter. This paper examines how to best inform competition policy of privacy issues. It does so by distinguishing between mandated privacy protection and higher levels of protection and then between situations where privacy is a competition parameter and those where it is not. In all instances, exchanges with privacy regulators would help the competition agency determination.

50

TOWARDS DATA PORTABILITY AND INTEROPERABILITY UNDER BRAZILIAN COMPETITION LAW: CRAFTING APPROPRIATE LEGAL STANDARDS FOR ABUSE OF DOMINANCE

By Victor Oliveira Fernandes

A crucial area of complementarity between competition and data protection law regimes is ensuring greater data mobility through data portability, interoperability, and open data standards in digital markets. The paper discusses how antitrust agencies would evaluate dominant platforms' strategies to prevent data interoperability as an abuse of dominance violation. It delves into this topic against the backdrop of Brazilian experiences. It argues that the critical choices to be made by antitrust authorities in these cases blur the limits of the intervention over the design of digital products. Some guidance on how to set the legal standards for these behaviors is provided to help with this challenge.

WHAT'S NEXT?

For January 2023, we will feature an Antitrust Chronicle focused on issues related to (1) **Robinson-Patman Act**; and (2) **Defining Platform Markets**.

ANNOUNCEMENTS

CPI wants to hear from our subscribers. In 2023, we will be reaching out to members of our community for your feedback and ideas. Let us know what you want (or don't want) to see, at: antitrustchronicle@competitionpolicyinternational.com.

CPI ANTITRUST CHRONICLES February 2023

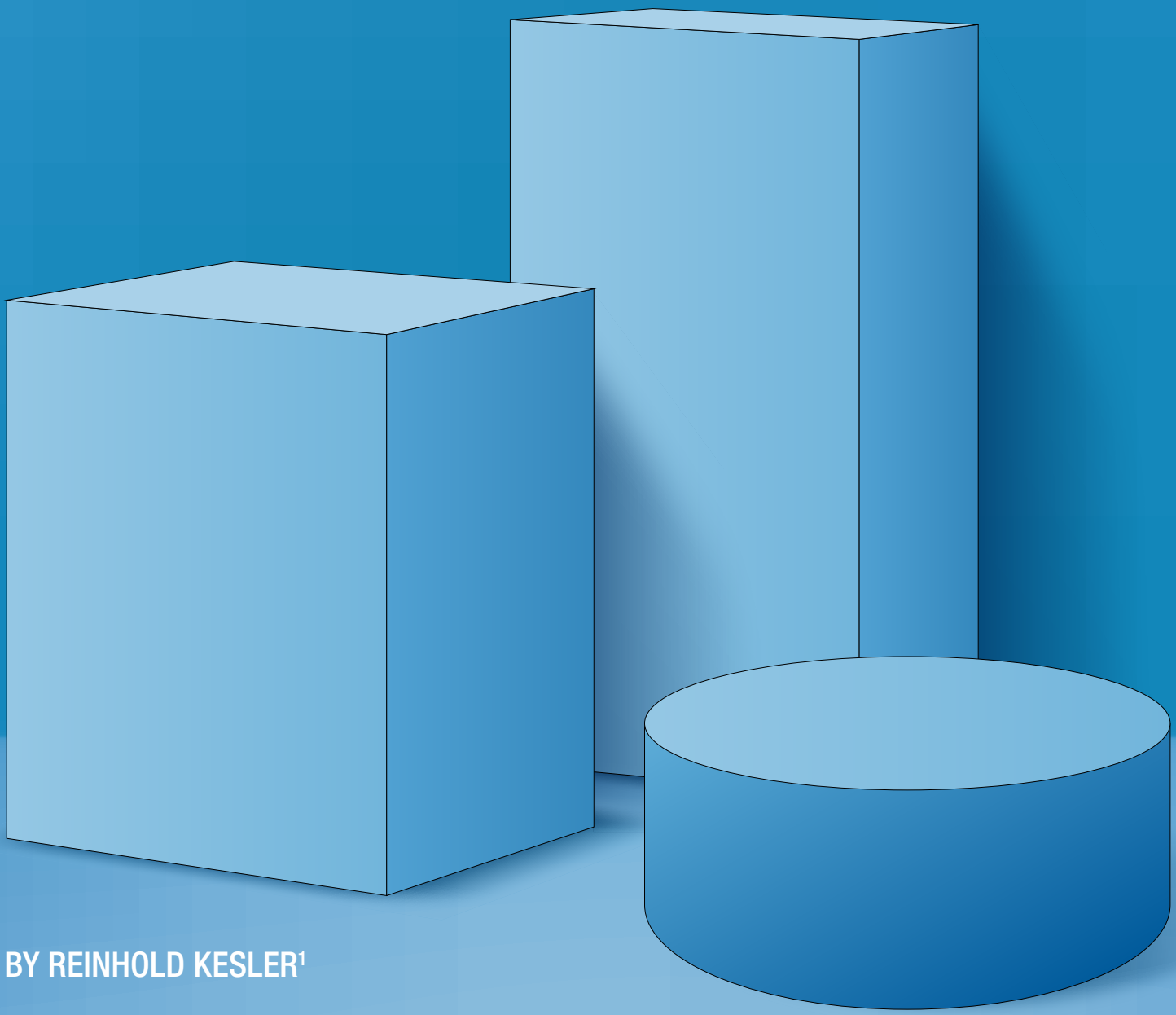
For February 2023, we will feature an Antitrust Chronicle focused on issues related to (1) **Mergers as Monopolization**; and (2) **White Collar Defense**.

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

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

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

DIGITAL PLATFORMS IMPLEMENT PRIVACY-CENTRIC POLICIES: WHAT DOES IT MEAN FOR COMPETITION?



BY REINHOLD KESLER[1]

1 Senior Research Associate, Department of Business Administration, University of Zurich, Plattenstrasse 14, CH-8032 Zurich, Switzerland. reinhold.kesler@business.uzh.ch.

I. INTRODUCTION

In recent years, several regulations worldwide came into effect that aim to better protect user privacy and, by this, set limits to the data economy that fuels many digital products and services, e.g., through targeted advertisements. Interestingly, digital platforms increasingly often enact privacy-centric policies, too. In this article, Apple's privacy change called App Tracking Transparency ("ATT") is studied as a representative example of such. Following a brief description of the policy, the remainder of the article primarily reviews scientific studies and investigations by competition authorities on the ATT while also relating to relevant research on privacy changes from the past to provide insights on the possible effects of Apple's privacy policy. While the focus of this article is on the implications the policy has for competition in Apple's mobile ecosystem, the platform's role and possible privacy benefits are also considered.

II. CASE IN POINT: APPLE'S APP TRACKING TRANSPARENCY ("ATT")

Today's primarily advertisement-funded Internet is increasingly often facing regulatory headwinds that set boundaries to the data economy at play. Regulatory efforts in place like the European General Data Protection Regulation ("GDPR") or those underway aim to better protect user privacy and mitigate the tracking of users that makes advertisements valuable. In that vein, digital platforms have already implemented or are about to introduce privacy-centric changes that foresee mitigating or the end of third-party tracking. Several studies in the past showed advertisement revenues to decrease with limited tracking abilities (see Section III for an overview). Wernerfelt et al. (2022), for a recent example, provide evidence for this so-called offsite data on users, which is shared across applications, to be important for advertisers on Meta.[2] The authors find costs to acquire new consumers through targeted advertisements to distinctively increase without access to such.

A case in point for a restriction on combining data across apps and websites is Apple's privacy change, called App Tracking Transparency. It came live with the iOS version 14.5 in April 2021 and involves a one-time prompt for each user of an app that explicitly asks for the consent to track outside the app in case the developer chooses to. Disallowing the tracking – and most users do so (until today) according to mobile analytics companies – leaves the app developer without the identifier for advertisers ("IDFA") of the respective user.[3] This identifier, however, serves to tailor advertising campaigns and to attribute the success of advertisement campaigns to specific users, thereby making advertisements more valuable. Consequently, both monetization from advertisements and acquiring (new) users through advertisements become more difficult in the post-ATT world. The relevance of this privacy change and the loss in tracking can already be seen anecdotally by reported revenues. The most popular firm to name is Facebook, with a loss of USD 10 billion in advertisement revenues in the year following the ATT,[4] while app developers disclosed decreases in the range of at least 15 to 20 percent (Competition and Markets Authority, 2022).[5]

This encourages a more systematic assessment of the impact of Apple's privacy change as one example of a platform-initiated privacy change. Specifically, it raises the question about the implications this policy has for competition, which is at the heart of the following sections.

III. CONSEQUENCES FOR COMPETITION

As outlined in Section II, Apple's policy limits business models revolving around targeted advertisements and puts the viability of business models at risk that rely on tracking through the IDFA. This affects market participants differently and potentially changes the competitive landscape, with winners and losers arising from the platform's privacy change. Following the ATT, changes in the business model by app developers may be expected. More specifically, a possible reduction in revenue along with rising costs may make app developers adjust their decisions to monetize and develop with the two main revenue sources being advertisements and in-app payments in the market for mobile applications.[6] The few studies that investigated the impact of the ATT along with previous related research shall provide some first insights onto the consequences for competition.

2 Wernerfelt, Nils, Anna Tuchman, Bradley Shapiro, & Robert Moakler, *Estimating the Value of Offsite Data to Advertisers on Meta* (Becker Friedman Institute for Economics Working Paper No. 114, 2022).

3 Flurry Analytics, *App Tracking Transparency Opt-In Rate - Monthly Updates* (May 2, 2022), https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/.

4 Kif Leswing, Facebook says Apple iOS privacy change will result in $10 billion revenue hit this year (February 02, 2022), https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html.

5 Competition and Markets Authority, *Mobile Ecosystems Market Study* (Final Report, 2022).

6 Flurry Analytics, *Are App Developers Shifting Revenue Models as Advertising Gets Challenged?* (August 13, 2020), https://www.flurry.com/blog/are-app-developers-shifting-revenue-models-as/.

As a starting point, Kraft et al. (2022) provide empirical evidence of a reduction in the tracking of users on Apple and consequentially also in apps' advertisement revenues following the ATT based on data from a provider enabling publishers to run mobile advertisement campaigns.[7] This is in line with previous studies showing a decrease in advertisement revenues when making it more costly or impossible to track users, be it through privacy policies (Tucker, 2012, 2014)[8] or disabling cookies (Goldfarb & Tucker, 2011; Johnson et al., 2020; Marotta et al., 2019).[9]

This pattern also holds for broader regulations such as the GDPR as found by several studies (Goldberg et al., 2022; Schmitt et al., 2021)[10] along with other research showing that data collection becomes more difficult (Aridor et al., 2022; Godinho de Matos & Adjerid, 2022).[11]

Given the decrease in advertisement revenue, a study that I am currently working on looks at whether app developers turn towards alternative revenue sources, which are payments.[12] Comparing apps on Apple with apps on Google, I find an effect, albeit small, that suggests app developers turn towards upfront payments and in-app payments following the ATT. Importantly, the impact is more pronounced for apps only active on Apple and those tracking through the identifier restricted, while apps born after the privacy change also include payments more often than pre-ATT.

A more drastic measure for the viability of a business model is the decision by app developers to enter or exit. In this regard, Li & Tsai (2022) find a decrease in the entry of new apps on Apple following the ATT enactment.[13] Relatedly, Kircher & Foerderer (Forthcoming) study the ban of targeted advertisement in the setting of children's games on Google's Play Store and find a substantial increase in app abandonment.[14] Following the GDPR, Janssen et al. (2022) also find a massive exit of apps on Google's Play Store, but the more consequential finding is the decrease in the entry of new apps, thereby quantifying a distinctive loss in welfare due to the unpredictability of success for apps.[15] Investments by venture capital in new and emerging firms, as another indicator for the viability of entrants, have been found to be reduced in the European technological sector relative to the United States after the GDPR enactment (Jia et al., 2021).[16] Finally, in the context of the GDPR, research also showed an increase in the market concentration of web technology services toward the main players, which comprise Google and Facebook (Batikas et al., 2022; Johnson et al., 2022).[17]

These various pieces of evidence for changes in monetization and development decisions, as well as the resulting impact on the competitive environment, already suggest the presence of winners in the wake of Apple's privacy change. Obviously, app developers less or not relying on tracking (via the restricted identifier) are hardly affected, which has already been shown for the likelihood to turn towards payments in my study.[18] However, less attention has been given to studying hypotheses made by industry people that the size of a firm along with its first-party

---

7 Kraft, Lennart, Bernd Skiera, & Tim Koschella, *Economic Impact of Apple's App Tracking Transparency (ATT)* (Working Paper, 2022).

8 Tucker, Catherine, *The Economics of Advertising and Privacy*, International Journal of Industrial Organization, 30 (3), 326–329 (2012); Tucker, Catherine, *Social Networks, Personalized Advertising and Privacy Controls*, Journal of Marketing Research, 51 (5), 546–562 (2014).

9 Goldfarb, Avi & Catherine Tucker, *Privacy Regulation and Online Advertising*, Management Science, 57 (1), 57–71 (2011); Johnson, Garrett, Scott Shriver, & Shaoyin Du, *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, Marketing Science, 39 (1), 33–51 (2020); Marotta, Veronica, Vibhanshu Abhishek, & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis* (Working Paper, 2019).

10 Goldberg, Samuel, Garrett Johnson, & Scott Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR* (Working Paper, 2022); Schmitt, Julia, Klaus M. Miller, & Bernd Skiera, *The Impact of Privacy Laws on Online User Behavior* (Working Paper, 2021).

11 Aridor, Guy, Yeon-Koo Che, & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR* (NBER Working Paper No. 26900, 2022); de Matos, Miguel Godinho & Idris Adjerid, *Consumer Consent and Firm Targeting After GDPR: The Case of a Large Telecom Provider*, Management Science, 68 (5), 3175–3973 (2022).

12 Kesler, Reinhold, *The Impact of Apple's App Tracking Transparency on App Monetization* (Working Paper, 2022).

13 Li, Ding & Hsin-Tien Tsai, *Mobile Apps and Targeted Advertising: Competitive Effects of Data Exchange* (Working Paper, 2022).

14 Kircher, Tobias & Jens Foerderer, *Ban Targeted Advertising in Apps? An Empirical Investigation of the Consequences for App Development*, Management Science (Forthcoming).

15 Janssen, Rebecca, Reinhold Kesler, Michael Kummer, & Joel Waldfogel, *GDPR and the Lost Generation of Apps* (NBER Working Paper No. 30028, 2022).

16 Jia, Jian, Ginger Zhe Jin, & Liad Wagman, *The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment*, Marketing Science, 40 (4), 661–684 (2021).

17 Batikas, Michail, Stefan Bechtold, Tobias Kretschmer, & Christian Peukert, *Regulatory Spillovers and Data Governance: Evidence from the GDPR*, Marketing Science, 41 (4), 235–441 (2022); Johnson, Garrett, Scott Shriver, & Samuel Goldberg, *Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR* (Working Paper, 2022).

18 Kesler, *supra* note 12.

data becomes increasingly important in a post-ATT world. Nevertheless, based on the above-mentioned studies, in the long-run, users will likely be faced with a different as well as potentially decreased choice set of available products and possibly weakened competition.

IV. DISCUSSING THE PLATFORM'S ROLE

Although there have been many privacy policies enacted in the past, a notable difference is that platforms now increasingly often motivate and implement such changes themselves, thereby (un-)intentionally deciding potential winners – including themselves. The ATT makes no exception, with policy makers being concerned with the implementation and the corresponding impact. For instance, the Competition and Markets Authority in the United Kingdom lists in its Mobile Ecosystems Market Study various factors:[19] It criticizes the choice architecture of the ATT prompt that is untested and different compared to personalized advertisements served by Apple. While it acknowledges the impact on targeted advertisements, it also states the concerns that the ATT potentially favors Apple's own advertisement services over others and protects Apple's market power for app distribution. Indeed, some of these potential double standards by Apple have been empirically studied by Kollnig et al. (2022) for apps in the United Kingdom app store.[20] They note that Apple makes and enforces app store policies with its definition of tracking exempting its own advertisement technology. The authors find Apple to have access to unique data, giving another edge to its market position and advertising service. Anecdotally, Apple's current expansion of its advertisement business is increasingly often seen as a self-serving practice following the implementation of the ATT. Examples found in news reports comprise the increasing importance of Apple Search Ads, additional advertisement spots within the app store, and numerous job listings devoted to advertisements.[21]

These observations are complemented by investigations of competition authorities in several countries, some of them based on complaints by publishers.[22] While the French competition authority did not block the policy change by Apple before the introduction, it chose to further investigate the case. The competition authority in Germany with its investigation on self-preferencing by Apple through ATT is also still pending.[23] The latter investigation raises concerns with respect to the combination of data as well as a potential reduction in user choice of apps financed through advertisements. In a broader context, regulations prohibiting self-preferencing of large digital platforms are on the horizon on both sides of the Atlantic. In the European Union, the Digital Markets Act will be enforced in 2024 at the latest, and Apple, as a gatekeeper, will thus face greater scrutiny. In the United States, the American Innovation and Choice Online Act is also well underway. Based on the concerns raised, it begs the question of whether the upcoming regulations may level the playing field.

V. ACCOUNTING FOR PRIVACY BENEFITS

Given the above-mentioned costs of privacy changes such as the ATT, it is still important to weigh them against the benefits of the policy change with regard to users' privacy for a complete evaluation of the policy. However, in the past, the value of user privacy has been found difficult to measure reliably. This was often attributed to the so-called privacy paradox, which corresponds to the dichotomy between (stated) privacy attitudes and actual privacy behavior.[24] As an illustrative example, valuations for allowing privacy-sensitive permissions for mobile applications inferred from observational data differ from the valuations of choice experiments by a factor of ten.[25] Acquisti et al. (2016) argue that the privacy paradox may arise due to various decision-making hurdles users typically face with asymmetric information, bounded rationality, and heuristics at play in the online setting.

19 Competition and Markets Authority, *supra* note 5.

20 Kollnig, Konrad, Anastasia Shuba, Max Van Kleek, Reuben Binns, & Nigel Shadbolt, *Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels*, FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency, p. 508–520 (2022).

21 Patrick McGee, *Apple plans to double its digital advertising business workforce* (September 04, 2022), https://www.ft.com/content/db21685b-d4dd-421d-95ac-980e9d40c05c.

22 Autorité de la Concurrence, *Targeted advertising: no urgent interim measures against Apple but the Autorité continues to investigate into the merits of the case* (March 17, 2021), https://www.autoritedelaconcurrence.fr/en/article/targeted-advertising-no-urgent-interim-measures-against-apple-autorite-continues.

23 Bundeskartellamt, *Bundeskartellamt reviews Apple's tracking rules for third-party apps* (June 14, 2022), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html.

24 Acquisti, Alessandro, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, Journal of Economic Literature, 54 (2), 442–92 (2016).

25 Kummer, Michael & Patrick Schulte, *When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications*, Management Science, 65 (8), 3470–3494 (2019); Savage, Scott J. & Donald M. Waldman, *Privacy Tradeoffs in Smartphone Applications*, Economics Letters, 137, 171–175 (2015).

Notably, in a more recent study, Bian et al. (2022) found consumers demand less with the disclosure of data collection by apps, which has been mandated by Apple since December 2020 in a fashion similar to nutrition labels consisting of the nature and purpose of data collected.[26] This specific context of privacy labels may show that the way how such information is brought to users seems to be important. In that regard, with ATT giving a straight-forward task and the majority of users opting out, this may be another instance that suggests a distaste for third-party tracking and an improvement in users' privacy.

Hence, it is important to assess how much value is necessary to offset welfare losses through the costs arising from such privacy changes. In future policy evaluations, these types of assessments would be helpful as privacy increasingly often becomes an antitrust issue in the last few years.

VI. CONCLUSION

In this article, Apple's App Tracking Transparency has been studied as an example of a privacy-centric policy enacted by a digital platform and its impact on competition. Following a review of the current state of research, several pieces of empirical evidence seem to suggest a weakened competitive environment in the long run as a result of Apple's privacy change undermining targeted advertisements. Importantly, the article highlights the platform's role in deciding potential winners – including themselves – with its implementation of the policy and stresses weighing the potential costs against the benefits through improved user privacy. All of this may serve as a starting point, both from a scientific and a policy perspective, on what to expect and consider about the upcoming privacy-preserving changes enacted by digital platforms.

26 Bian, Bo, Xinchen Ma, & Huan Tang, *The Supply and Demand for Data Privacy: Evidence from Mobile Apps* (Working Paper, 2022).

HARMING COMPETITION AND CONSUMERS UNDER THE GUISE OF PROTECTING PRIVACY: REVIEW OF EMPIRICAL EVIDENCE

BY D. DANIEL SOKOL & FENG ZHU[1]

1 Carolyn Craig Franklin Chair in Law and Business and Professor, USC, and MBA Class of 1958; Professor of Business at HBS respectively. We gratefully acknowledge support from Meta Platforms, Inc. in funding this analysis. The views expressed here are solely our own.

I. INTRODUCTION

Apple proposed the new "App Tracking Transparency" ("ATT") policy in November 2020, and required all apps to have this feature enabled on April 26, 2021, which was the beta release of iOS 14.5. The policy prohibits apps from engaging in any activity that Apple defines as "tracking" unless the apps prompt users for "permission to track [them] across apps and websites owned by other companies" and users explicitly opt in to "tracking."[2]

The policy was framed as a privacy-protecting measure. In a prior essay,[3] we identified that this policy actually masked anti-competitive conduct under traditional antitrust theories. Further, we suggested that the policy would have the pernicious effects of enhancing the dominance of iOS among mobile-operating systems ("OSs") and the dominance of its own apps and services within the iOS ecosystem, while reducing consumer choice and devastating the free-app ecosystem enabled by personalized advertising.

The logic is as follows: Since data tracking is important to ad-based monetization used by free and freemium apps, privacy-protection policies that prohibit data tracking will harm the profitability of such business models. In the Apple iOS case, developers further would be put at disadvantage by Apple's asymmetric implementation of its policy on third-party apps versus its own apps. We hypothesized that developers may have to exit the market due to lack of financing, switch from ad-based to fee-based monetization, or turn to Apple's own aggregation services. Among those affected, small and new firms (advertisers and developers) would suffer the most. Consumer choice would be restricted, and consumers would be steered towards Apple's own apps and services. As consumers would have a higher switching cost to leave for another platform, this would reinforce the dominance of iOS in the mobile ecosystem.

As a follow up from our previous essay, which provides more theoretical explanations on how the ATT policy may harm competition and consumers, this essay provides an overview of the empirical evidence examining both Apple's new ATT policy and other similar privacy-protection regulations or programs (e.g. the ePrivacy Directive and General Data Protection Regulation ("GDPR") in Europe, and the California Consumer Privacy Act in the U.S. ("CCPA") in bolster our argument above. We conclude that the empirical findings generally support the concerns that we raised in our prior essay. Our concerns about the anti-competitive effects of privacy-related policies should be considered when evaluating any privacy-protection policy.

II. DATA TRACKING IS IMPORTANT TO PERSONALIZED ADVERTISING AND AD-BASED MONETIZATION

Mobile device users nowadays have become accustomed to free apps and content that come with ads. Ad-based monetization is an important part of free and freemium business models,[4] which currently accounts for a significant share of apps available on both iOS and Android platforms. Most of these apps use personalized advertising.

The effectiveness of personalized advertising, and in turn the profitability of ad-based monetization, relies critically on the ability of data tracking. With more accurate data on consumers' preferences and interests, it is easier for advertisers to send ads that are more effective to consumers and achieve a higher conversion rate. With more accurate data on which ads lead to valuable events such as clicks, downloads and/or actual sales, advertisers can more efficiently measure and compare the performances of different advertising strategies and adjust accordingly.[5]

2 *User Privacy and Data Use*, APPLE, https://developer.apple.com/appstore/user-privacy-and-data-use/ [https://perma.cc/CTC5-9XQC] (last visited May 3, 2021) ("Tracking refers to the act of linking user or device data collected from your app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers."). We use tracking because it is the academic term though it has an ominous sound to it.

3 D. Daniel Sokol & Feng Zhu, *Harming Competition and Consumers Under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates*, 107 Cornell L. Rev. Online 101 (2022).

4 According to an AdColony survey, non-gaming apps derive 66 percent of their revenue, and gaming apps derive 63 percent of their revenue, from advertising. See Dean Takahashi, *AdColony: 89% of Mobile App and Game Publishers Use Video Ads*, VENTUREBEAT (Feb. 12, 2020), https://venturebeat.com/2020/02/12/adcolony-89-of-mobile-app-and-gamepublishers-use-video-ads/ [https://perma.cc/6H6R-DRAY].

5 See Catherine E. Tucker, *The Economics of Advertising and Privacy*, 30 Int'l J. Indus. Org. 326, 326 (2012); Avi Goldfarb & Catherine E. Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 Mrktg. Sci. 389, 402 (2011); Bharat N. Anand & Ron Shachar, *Targeted Advertising as a Signal*, 7 Quantitative Mrktg. & Econ. 237, 238–39 (2009).

The reliance of effective advertising on data tracking has been confirmed by empirical findings.[6] Goldfarb & Tucker evaluated how the enactment of the ePrivacy Directive in 2003 and 2004 affected the performance of ad campaigns in the European Union ("EU"). They found that, after the ePrivacy Directive was passed, advertising effectiveness decreased on average by around 65 percent in Europe relative to other countries.

Further, Aziz & Telang[7] utilized a dataset from a large digital advertising firm for one large retargeting campaign for a multi-category e-commerce firm on a randomly selected day. The authors considered six different predictive models, each including more variables from a user's cookie information than the previous one and showed that the accuracy of prediction of purchases increased as more variables were included for prediction. The authors concluded more intrusive information for targeting could substantially increase ad effectiveness and lead to more potential purchases.

Finally, Kummer & Schulte[8] examined 300,000 apps obtained from the Google Play Store in 2012 and 2014 and concluded that cheaper apps required more privacy-sensitive permissions, which remained robust whether the inference is based on the cross-section snapshot, the panel data or a manually constructed "app siblings" dataset consisting of a free and a paid version of the same app.

III. PRIVACY-PROTECTION POLICIES MAKE DATA TRACKING HARDER AND HURT PERSONALIZED ADVERTISING

The implementation of privacy-protection policies limits the ability of data tracking for apps, and in turn the profitability of personalized advertising. This would hurt advertisers, developers, as well as consumers, who might have benefited from the ad-based monetization business models. We identify the issues each of these harmed groups as we identify each of how our predictions of the ATT policy played out.

For advertisers, personalized advertising is an efficient way for businesses, particularly small businesses, to connect their products and services with consumers who actually desire them.[9] Targeted advertising is critical for the survival of small businesses, and it encourages new entrants into the market, as they can effectively market their products even with a small marketing budget.[10] For developers, personalized advertising provides an alternative way to monetize and promote their apps with fewer constraints, as compared to Apple's 15 – 30 percent commission for fee-based or subscription-based business models.[11]

The empirical evidence has shown that, when data tracking is hampered by privacy-protection policies, and personalized advertising becomes less effective and efficient, both advertisers and developers experience a significant drop in revenue.[12]

---

6 See Avi Goldfarb & Catherine E. Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MKTG. SCI. 389, 402 (2011); See Catherine E. Tucker, *The Economics of Advertising and Privacy*, 30 Int'l J. Indus. Org. 326, 326 (2012); Michael Kummer & Patrick Schulte, *When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications*, 65 Mgmt. Sci. 8 (2019).

7 Arslan Aziz & Rahul Telang, What Is a Digital Cookie Worth?, available at https://ssrn.com/abstract=2757325.

8 Kummer & Schulte, *supra* note 6.

9 See J. Howard Beales & Jeffrey A. Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, NAVIGANT ECON. (Jan. 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2421405 (finding where more information about users is available, transaction price increased by at least 60 percent relative to average price).

10 See e.g. Victoria Turk, *How Glossier Turned Itself into a Billion-dollar Beauty Brand*, WIRED (Feb. 6, 2020), https://www.wired.co.uk/article/how-tobuild-a-brand-glossier [https://perma.cc/W2Z4-VCAE]; Yuyu Chen, *How Brooklinen used word-of-mouth to grow a $15 mil. bedding business*, DIGIDAY (July 20, 2016), https://digiday.com/marketing/brooklinen-used-word-mouth-grow-15m-bedding-business/ [https://perma.cc/J8Z3-TFUN].

11 See Ian Carlos Campbell & Julia Alexander, *A Guide to Platform Fees*, THE VERGE, https://www.theverge.com/21445923/platform-fees-apps-gamesbusiness-marketplace-applegoogle#:~:text=Apple%20App%20Store%3A%2030%20percent,15%20percent%20after%20one%20year [https://perma.cc/Y2DN-ADND] (last visited Mar. 28,2022); *App Store Small Business Program*, APPLE, https://developer.apple.com/app-store/small-business-program/ [https://perma.cc/DTC3-88LZ] (last visited May 3, 2021) (discussing Apple's 15 percent commission on paid apps and in-app purchases for existing developers who made up to $1 million in proceeds in 2020).

12 See Garrett A. Johnson, *The Impact of Privacy Policy on the Auction Market for Online Display Advertising*, Managerial Mtkg. eJournal (2013); Garrett A. Johnson et al., *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, 39 Mktg. Sci. 1 (2020); Miguel Alcobendas et al., *The Impact of Privacy Measures on Online Advertising*, SSRN 3782889 (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782889; Samuel Goldberg et al., *Regulating Privacy Online: An Economic Evaluation of the GDPR*, SSRN 3421731 (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421731.

IV. DEVELOPERS SUFFER FROM APPLE'S ASYMMETRIC IMPLEMENTATION OF PRIVACY-PROTECTION POLICIES

The iOS privacy policy update put developers at a large disadvantage due to the different privacy-protection policies faced by third-party apps and Apple's own apps.

For third-party apps, users must explicitly opt in to "tracking" on the prompt screen. The term "tracking" is broadly defined by Apple to include behaviors other than following users' activity throughout the internet, and extends well beyond what most users would consider "tracking." For example, Apple's definition of "tracking" includes displaying targeted ads "based on user data collected from apps and websites owned by other companies," sharing email lists or other IDs with a third-party ad network that uses that information to retarget, and "[p]lacing a third-party SDK in your app that combines user data from your app with user data from other developers' apps to target advertising or measure advertising efficiency, even if you don't use the SDK for these purposes."[13] Moreover, even if consumers have previously consented to data use through an alternative channel by the advertiser or developer, data tracking is still restricted by Apple as long as the consumer interacts with the app on the iOS platform.

Meanwhile, the opt-in requirement does not apply to Apple's own apps and services.[14] Consumers are "opted in" to Apple's tracking by default; even though Apple also use consumers' data collected in other companies' apps for personalized advertising.[15] The user has to manually opt out through an option buried deeply under a host of other settings, which Apple refers to as a more positive "personalized advertising" instead of the more ominous "tracking."

Studies have shown that consumers are less likely to consent to their data being shared if they believe that their privacy is protected.[16]

Applying the same logic, and taking into consideration Apple's introduction of a misleading prompt, the opt-in rate to "tracking" would be even lower for third-party apps. In fact, four months after the iOS 14.5 update at which the ATT policy was enforced, the worldwide opt-in rate across all apps was 21 percent (and 15 percent in the U.S.), that across apps with prompts was 23 percent (and 16 percent in the U.S.), and the share of users who cannot track by default was 4 percent (and also 4 percent in the U.S.).[17] The data is also consistent with two ex ante estimates which predicted that as many as 80 – 85 percent of users will choose not to opt in.[18]

A. Many Developers Quit Developing Apps Due to Lack of Financing

How do developers respond to the new policy? Some developers, especially those in the startup stage that are mainly financed by either venture capital ("VC") investments or revenues from displaying ads, may have no choice but to quit developing their apps, following a reduction in advertising budgets and lack of funding opportunities from VCs. The exit of startup apps and lack of new entrants suggest substantial costs in foregone innovation associated with the privacy-protection policies.

The ePrivacy Directive and GDPR program in the EU provided us with ample evidence of this possibility that we articulated in our prior essay. For example, an IAB study predicted a reduction in advertising budgets for display advertising by 2020 between 45 percent and 70

13 See *User Privacy and Data Use*, APPLE, https://developer.apple.com/appstore/user-privacy-and-data-use/ [https://perma.cc/CTC5-9XQC] (last visited May 3, 2021).

14 See *generally* Punam Anand Keller et al., *Enhanced Active Choice: A New Method to Motivate Behavior Change*, 21 J. Consumer Psych. 376 (2011).

15 See *Apple Advertising & Privacy*, APPLE, https://www.apple.com/legal/privacy/data/en/apple-advertising/ [https://perma.cc/9WDB-GPUG] (last visited Mar. 28, 2022) .

16 See Alessandro Acquisti et al., *What is Privacy Worth?*, 42 J. Legal Stud. 249, 252 (2013) ("In our experiment, subjects were five times more likely to reject cash offers for their data if they believed that their privacy would be, by default, protected than if they did not have such a belief.").

17 See Estelle Laziuk, *iOS 14 Opt-in Rate - Weekly Updates Since Launch,* Flurry (Sept. 6, 2021), https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/ [https:// https://perma.cc/KEJ9-6XMM]

18 See H. Judiciary Subcomm. On Antitrust, Commercial, and Administrative Law, 117th Cong. 6, *Reviving Competition, Part 1: Proposals to Address Gatekeeper Power and Lower Barriers to Entry Online:* (2021) (statement of J. Thorne), https://docs.house.gov/meetings/JU/JU05/20210225/111247/HHRG-117-JU05-Wstate-ThorneJ-20210225.pdf [https://perma.cc/MU36-5SES]; s*ee also Dean Takahashi, The DeanBeat: What's at Stake in Apple's Potentially Apocalyptic IDFA Changes*, Venturebeat (Oct. 9, 2020), https://venturebeat.com/2020/10/09/the-deanbeat-whats-at-stake-in-applespotentially-apocalyptic-idfa-changes/ [https://perma.cc/6KE7-4BPV] (noting that "most observers predicted that no more than 20% of users would opt-in"); Andrew Blustein, *Apple Has Finally Implemented Its Privacy Overhaul, Here's What You Need to Know*, ADWEEK (Apr. 26, 2021), https://www.adweek.com/programmatic/apple-has-finally-implemented-itsprivacy-overhaul-heres-what-you-need-to-know/ [https://perma.cc/V8BBQYYJ] (Although the Adweek preliminary study estimates 32 percent opt-in rates, it found lower rates, nearly 20 percent, for gaming apps.).

percent as a combined effect of GDPR and ePrivacy Directive.[19] In addition, both programs have had negative effects on VC investments, which were particularly pronounced for newer, data-related, and business-to-consumer ("B2C") ventures.[20] Lastly, following the iOS 14.5 privacy policy update, Li & Tsai have also documented a similar pattern of apps that are more inactive and fewer new startup apps.[21]

V. MANY DEVELOPERS SWITCH FROM AD-BASED FEE-BASED MONETIZATION

Developers may also switch from ad-based monetization to fee-based monetization. However, apps that monetize through download fees, subscription fees or in-app purchases ("IAPs"), will all be subject to Apple's 15 – 30 percent commission, thus increasing developers' costs.[22] Although consumers value the free apps and content, once the app developers shift from ad-supported to paid models, consumers may be willing to pay a modest fee for certain apps, but are unlikely to pay a fee for each and every app they use.[23] Thus, not all apps will be able to make this shift. Empirical evidence from the iOS privacy policy update also showed that, in general, the new privacy policy reinforced the trend toward more fee-based monetization, and the impact was more prevalent among new apps.[24]

Two papers specifically focus on the impacts of ATT. The first is Kesler,[25] which considered the impact of Apple's recent privacy policy on app monetization. The author collected monthly web-scraped data from February 2021 to December 2021 of 583,384 apps on iOS and 901,182 apps on Android. The iOS apps were chosen by scraping top ranked apps from App Annie, and gathering other apps by the same developer and similar apps suggested by the App Store, while the Android apps were chosen based on a panel from Janßen et al.[26] and extended by including similar apps. For each app, the authors collected information on its monetization, its reliance on Apple (proxied by whether single-homing), and its reliance on data tracking. Both the before-and-after analysis and the DID analysis of iOS apps against Android apps show that the new privacy policy reversed the preceding negative trend for the presence of paid apps and reinforced the existing trend toward more in-app payments. Although the impact was small on average, it was more prevalent among apps relying on Apple, relying on user tracking, or belonging to younger cohorts.

VI. SMALL AND NEW FIRMS (ADVERTISERS AND DEVELOPERS) SUFFER THE MOST

Among those businesses affected by the implementation of privacy-protection policies, small advertisers and developers that recently or are about to enter the market usually suffer the most.

Small businesses rely heavily on personalized advertising.[27] With limited marketing budgets and a very specific audience, it is critical for small advertisers to reach prospective customers efficiently and effectively through personalized advertising.[28] Apple's new privacy policy update, which impairs small advertisers' ability to do so, will thus have a particularly pronounced effect on their survival.

19 See Christian Hildebrandt & René Arnold, *Economic Impact of the ePrivacy Regulation on Online Advertising and Ad-based Digital Business Models*, WIK, at II (Nov. 2017), https://www.wik.org/fileadmin/Studien/2017/WIK_ePrivacy_study_ENGLISH.PDF (last visited Nov. 8, 2022) [https://perma.cc/BG59-RNPN].

20 Anja Lambrecht, *E-Privacy and Venture Capital Investments in the EU* (2017); Jian Jia et al., *The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment*, 40 Mktg. Sci. 4 (2021).

21 Ding Li & Hsin-Tien Tsai, Mobile Apps and Targeted Advertising: Competitive Effects of Data Exchange, available at https://ssrn.com/abstract=4088166.

22 See Sarah Perez, *Apple lowers commissions on in-app purchases for news publishers who participate in apple news*, TECHCRUNCH, https://techcrunch.com/2021/08/26/apple-lowers-commissions-on-in-apppurchases-for-news-publishers-who-participate-in-apple-news/ (last visited Mar. 28, 2022) [https://perma.cc/7PQT-8NNM].

23 Network Advert. Initiative, *Consumer Survey on Pricing and Digital Advertising* at 4, 6-7 (Oct. 22, 2019), https://www.networkadvertising.org/sites/default/files/final_nai_consumer_survey_paper_22oct2019.pdf [https://perma.cc/H3TE-WVRH].

24 Reinhold Kesler, *The Impact of Apple's App Tracking Transparency on App Monetization*, SSRN 4090786 (2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4090786.

25 *Id.*

26 Rebecca Janßen, *GDPR and the lost generation of innovative apps* (No. w30028), National Bureau of Economic Research, available at https://www.nber.org/papers/w30028.

27 See Deloitte LLP, *Digital Tools in Crisis and Recovery – Small and Medium Business Report*, at 33 (Oct. 2020), https://about.fb.com/wpcontent/uploads/2020/10/Deloitte-Digital-Tools-in-Crisis-and-Recovery-SMBReport-Oct-2020.pdf [https://perma.cc/Y4RK-B44V] (found that personalized advertising is especially important for SMBs seeking to identify and win new customers: "US SMBs who reported using targeted advertising on social media were twice as likely to target new customers.").

28 See Erin Egan, *A Path Forward for Privacy and Online Advertising*, FACEBOOK (Oct. 2, 2020), https://about.fb.com/news/2020/10/a-path-forward-for-privacy-andonline-advertising/ [https://perma.cc/CT72-T6LS] (removing personalization from the ads delivered on off-Facebook apps resulted in "a greater than fifty percent drop in revenue for mobile app install campaigns"); Dan Levy, *Speaking Up for Small Businesses*, FACEBOOK (Dec. 16, 2020), https://about.fb.com/news/2020/12/speaking-upfor-small-businesses/ [https://perma.cc/MKW8-ZM5E] (noting findings that "without personalized ads powered by their own data, small businesses could see a cut of over 60 percent of website sales from ads").

Several aforementioned empirical analyses have noticed the particular harm done to small and new firms. Goldberg et al.[29] found that smaller e-commerce sites saw twice the decline in recorded revenue than larger sites, due to that they were harder to obtain consent from consumers. Jia et al.[30] showed that the negative post-GDPR effects were particularly pronounced for newer ventures. In addition, Canayaz et al.[31] noted that voice-AI firms with small customer bases were hit the hardest under CCPA, due to a low ability to collect in-house data and high reliance on externally purchased data.

Similarly, small developers are also in a worse position. When there is a reduction in advertising budgets and funding opportunities, small developers are even less likely to secure a way to finance their apps. In addition, because consumers are willing to maintain only a limited number of stand-alone app subscriptions, it is also unlikely for small developers to successfully switch to fee-based monetization. One last alternative for small developers is to distribute apps through Apple's aggregation services, such as Apple News+ (for news apps) and Apple Arcade (for games).

VII. CONSUMERS TURN TO APPLE'S OWN APPS AND SERVICES AND HAVE HIGHER SWITCHING COSTS

Ad-supported apps are an important part of inter-OS competition, as they lower the barriers for consumers to switch between mobile OSs. However, as Apple rolled out its new privacy policy, developers have been forced to switch away from ad-based monetization, and either quit developing their apps, or move towards fee-based monetization, or distribute apps through Apple's aggregation services. Consumers are thus steered towards either paid apps (which often require users to repurchase upon switching to a new mobile OS) or Apple's own apps (which are not available on another mobile OS).[32] Furthermore, as paid apps are subject to Apple's 15 – 30 percent commission, the third-party apps are even less competitive against Apple's own apps. In the end, Apple's new privacy policy helps to lock consumers into iOS by building a moat around them with a combination of fee-based apps, Apple's own apps and services and a host of other restrictions,[33] and make switching to another mobile OS, such as Android, even harder.

VIII. PRIVACY-PROTECTION POLICIES BENEFIT LARGE FIRMS AND INCREASE MARKET CONCENTRATION

On net, strong privacy-protection policies benefit large firms like Apple and increase market concentration. Such a phenomenon is a common theme in empirical studies. For example, among the aforementioned empirical studies: Alcobendas et al.[34] showed that the ban of third-party cookies in ad auctions would benefit bidders (advertisers) with an information advantage (analogue to Apple's own apps and services enjoying

29 *Supra* note 12.

30 *Supra* note 20.

31 Mehmet Canayaz et al., Consumer Privacy and Value of Consumer Data, Swiss Finance Institute Research Paper No. 22-68, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3986562.

32 See JR Raphael, *iPhone to Android: The Ultimate Switching Guide*, COMPUTERWORLD (Feb. 7, 2020), https://www.computerworld.com/article/3218067/how-to-switch-fromiphone-to-android-ultimate-guide.html (explaining that iPhone apps will not automatically transfer over to Android and apps paid for on iOS will have to paid for again on Android) [https://perma.cc/N4ZV-S69D].

33 For instance, Apple faces charges from the European Commission stemming from Spotify's 2019 complaint about Apple's unfair treatment of Spotify's streaming service on the App Store and large commissions, which led Spotify to "'artificially' increase monthly subscriptions for its premium service to cover the extra costs." See Aoife White, *Apple May Face Antitrust Complaint as EU Steps Up Spotify Probe*, BLOOMBERG (Mar. 4, 2021), https://www.bloomberg.com/news/articles/2021-03-04/apple-may-faceantitrust-complaint-as-eu-steps-up-spotify-probe [https://perma.cc/PS5RE JHF3]; *see also Antitrust: Commission Opens Investigations into Apple's App Store Rules*, EUR. COMM'N, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073 [https://perma.cc/N4VD-A7FW] (last visited Mar. 28, 2022)]. Apple has also received criticism for its app store policies that have prevented users from using cloud gaming services on iOS. See Tom Warren, *Facebook Slams Apple's App Store Policies, Launches Facebook Gaming on iOS Without Games*, THE VERGE (Aug. 7, 2020), https://www.theverge.com/2020/8/7/21358355/facebookapple-app-store-policies-comments-facebook-gaming-ios [https://perma.cc/YP3L-9XXA]. There are also reports that the DOJ is investigating Apple's "Sign in With Apple" button, which Apple requires for all developers who have other "sign in with" options. See Josh Sisco, *Apple's App Sign-in Button Becomes Hot-Button Issue in U.S. Antitrust Probe*, THE INFO. (Feb. 23, 2021), https://www.theinformation.com/articles/apples-app-sign-inbutton-becomes-hot-button-issue-in-u-s-antitrust-probe [https://perma.cc/BF8F-LBZ2].

34 *Supra* note 12.

an advantage against third-party apps in iOS). Schmitt et al.[35] found that popular websites suffered less in terms of user quantity and usage intensity from the enactment of GDPR, suggesting that GDPR might have increased market concentration. Johnson et al.[36] found in the web technology market that, as post-GDPR websites cut on their usage of vendors, they also moved towards Google and Facebook, which drove increased concentration. Peukert et al.[37] noted that Google lost relatively less and significantly increased market share in important markets such as advertising and analytics post-GDPR.[38]

IX. CONCLUSIONS

Apple's new privacy policy offers consumers a binary "choice" for privacy control on third-party apps: either "privacy" or "no privacy." Nonetheless, empirical evidence suggests that consumers are often better off if they are given more privacy controls. For example, Tucker[39] found in a natural experiment of ad campaigns on Facebook that, after Facebook's change in its privacy interface, which included aggregating all privacy settings into one simple control and making it easier for users to opt out from third-party applications accessing their personal information, consumers had an increased sense of control, and the personalized ads were more effective. Further, Godinho de Matos & Adjerid[40] found in their experiment with TELCO on consent elicitation that, consumers provided more allowance on data after consumer consent was elicited, allowing firms' reliant on consumers' personal information to improve outcomes.

The overall empirical record on competition and privacy scholarship as well as ATT specific scholarship lead to the conclusions that: (1) competition and privacy can be at odds; and (2) that Apple's ATT policy has made app developers, particularly small and new firms, worse off. The ATT policy has done so by masking anti-competitive conduct under the guise of privacy protection.

35 Julia Schmitt et al., *The Impact of Privacy Laws on Online User Behavior* (October 1, 2021). HEC Paris Research Paper No MKG-2021-1437, available at https://ssrn.com/abstract=3774110.

36 Garrett Johnson et al., *Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR* (November 14, 2022), available at https://ssrn.com/abstract=3477686.

37 Christian Peukert et al., *Regulatory Spillovers and Data Governance: Evidence from the GDPR*, 41 Mrktg. Sci. [_] (2022 forthcoming).

38 See WHOTRACKSME, *GDPR – What happened?*, (Sept. 3, 2018) https://whotracks.me/blog/gdpr-what-happened.html [https://perma.cc/9DWC-45TY] ("Google's advertising services have maintained their market share, while other advertisers across the board have lost reach. There could be several reasons to explain Google's favorable state post GDPR: 1. Resources thrown at compliance: Google and other big companies have had significant resources dedicated to compliance. 2. Google acts in the capacity of a gatekeeper, hence it is conceivable to assume it may have used that position in punitive ways. Reports indicate that Google could have encouraged publishers to reduce the number of AdTech vendors. 3. Websites owners trying to minimize their exposure opt for 'safer choices', dropping smaller advertisers that may have a harder time proving compliance.").

39 Catherine E. Tucker, *Social Networks, Personalized Advertising, and Privacy Controls*, 51 5 J. Mrktg. Res. 546 (2014).

40 Miguel Godinho de Matos & Idris Adjerid, *Consumer consent and firm targeting after GDPR: The case of a large telecom provider*, 68 Mgmt. Sci. 333 (2022).

EFFECTS OF GOVERNMENT SURVEILLANCE ON COMPETITION

BY ALEX MARTHEWS & CATHERINE TUCKER[1]

1 Alex Marthews is National Chair at Restore the Fourth, a nonprofit Fourth-Amendment advocacy organization. Catherine Tucker is Sloan Distinguished Professor of Management at MIT Sloan.

Following on from the shock of the Snowden revelations, it is now well established empirically that chilling effects from government surveillance and other privacy violations exist, that they can at least sometimes be quantified, and that significant proportions of citizens in many countries both describe themselves as being harmed by them, and alter their actual behavior in response.[2] What is less well established or understood is how a government's interest in maintaining mass surveillance programs could affect competition. This article studies this question.

I. GOVERNMENT SURVEILLANCE MAY LEAD TO A NATURAL TENDENCY TO FAVOR INCUMBENTS

History offers substantial reason to suspect that governments conducting surveillance may well actively prefer long-term, stable partnerships with incumbent firms, over an environment of small, intensely competing firms with a rapidly changing cast of senior managers. For example, the U.S. National Security Agency is reported to have developed over the years a "highly collaborative," "extraordinary, decades-long partnership" with AT&T codenamed "FAIRVIEW," and a further partnership with Verizon and MCI codenamed "STORMBREW," to surveil Internet traffic passing through their servers.[3]

Early literature on the topic of the interaction between surveillance concerns and antitrust speculates about an opposite concern: That expanding government surveillance powers might enable the government to surveil firms, uncover evidence of anti-competitive practices, and result in more severe antitrust enforcement.[4] This does not seem to have occurred, perhaps because courts have construed narrowly the PATRIOT Act's expansion of DOJ wiretapping powers in the area of antitrust investigations.

However, there is evidence in that the fears expressed in this article may have come true on occasions. In litigation documents reported on in 2007,[5] for example, the former CEO of Qwest, an AT&T and Verizon competitor, alleged that the U.S. government withdrew promised contracts as retaliation for Qwest's refusal to cooperate with unlawful surveillance requests in February 2001, placing Qwest at a competitive disadvantage. The telecommunications companies' cooperation with government surveillance programs has been the subject of considerable litigation from 2006 through to 2022.[6] If these allegations were true, then, the U.S. government acted to limit the set of telecommunications providers serving U.S. customers to the set of firms who had agreed to cooperate with illegal executive branch surveillance of their users.

Another example is given by the fact that in 2014, Lavabit was a small email provider that marketed itself as providing particularly private and heavily encrypted email services, with a premium offering that offered the highest level of encryption.[7] This attracted Edward Snowden to sign up to their service. After he came forward, the FBI approached Lavabit's CEO, Ladar Levison, with a 'pen register' order for the metadata for Snowden's account. Levison explained that the account-level encryption Snowden had paid for made it impossible for Lavabit to read the metadata on his email. The FBI then ordered him to disclose his "developer-level keys," decrypting all Lavabit accounts so that they could reach Snowden's. Eventually, Levison provided the keys in a form the FBI could easily read, but chose to shut down his service the next day, rendering those keys useless, rather than to "become complicit in crimes against the American people." Again, taken by the executive branch of the U.S. government - that had the effect of limiting the options available to U.S. consumers, to offerings that enabled law enforcement decryption of content.

---

2 See Marthews, A. & Tucker, C. E., "Government surveillance and internet search behavior. SSRN." (2014); Marthews, A. & Tucker, C. E., The Impact of Online Surveillance on Behavior (June 18, 2017). Cambridge Handbook of Surveillance Law, available at SSRN: https://ssrn.com/abstract=3167473; Marthews, A., & Tucker, C. E., "Privacy policy and competition." Brookings Paper (2019); Penney, J. W. (2016), "Chilling effects: Online surveillance and Wikipedia use," Berkeley Technology Law Journal 31, 117; Penney, J. W. (2017), "Internet surveillance, regulation, and chilling effects online: A comparative case study," Internet Policy Review; Stoycheff, E. (2016), "Under surveillance: examining Facebook's spiral of silence; effects in the wake of NSA internet monitoring," Journalism & Mass Communication Quarterly 93(2), 296–311.

3 See Angwin, J., Larson, J., Moltke, H., Poitras, L., Risen, J. & Savage, C., "AT&T Helped U.S. Spy on Internet on a Vast Scale," *New York Times*, August 15, 2015, available at https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html, accessed December 7, 2022.

4 See Donald, E. S., *Electronic Surveillance and Antitrust Investigations: The Effect of the Reauthorized Patriot Act*, 41 U.C. Davis L. Rev. 387 (2007).

5 See Eggen, D. & Nakashima, E., "Former CEO Says U.S. Punished Phone Firm," available at https://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485.html, accessed December 7, 2022.

6 For an overview, see Cohn, C., "EFF's Flagship Jewel v. NSA Dragnet Spying Case Rejected by the Supreme Court," June 13, 2022, available at https://www.eff.org/deeplinks/2022/06/effs-flagship-jewel-v-nsa-dragnet-spying-case-rejected-supreme-court, accessed December 7, 2022.

7 Franceschi-Bicchierai, L., "Lavabit's Forgotten Encryption Fight Looms Over the Apple Case.," March 18,, 2016, *Vice*, available at https://www.vice.com/en/article/gv5vg3/lavabit-snowden-forgotten-encryption-fight-looms-over-the-apple-fbi-case, accessed December 12, 2022.

By contrast, in February 2016, the FBI brought a court case against Apple, to force Apple to take steps to decrypt the work phone of the shooter in the San Bernardino massacre. Apple refused, and litigated the matter; the FBI then withdrew the request, having found a third-party provider of software that could decrypt the phone. The FBI found nothing of investigatory significance on the phone.[8] Crucially, however, the FBI, dealing with a globe-spanning tech firm with hundreds of millions of customers, did not ask Apple for its developer-level keys, which would have decrypted all Apple traffic.

In other words, larger firms, all else being equal, are better equipped to manage and resist public government surveillance demands, via court orders or other data requests, on the "front end" than small firms are. The risk to large firms of refusing such an order is not existential in the way that it can be for small firms like Lavabit. Smaller firms may find it harder than incumbents to respond to general privacy regulations, especially those that require the implementation of a consumer consent-based privacy framework.[9] In that sense, it seems clear that large telecommunications firms like AT&T and Verizon have the capacity to resist front-end government surveillance demands, even if it appears that in fact those firms have chosen instead to form a deep collaboration with the U.S. government.

There may be a strategic element to these kinds of interactions. A small firm like Lavabit may not have a large number of users in which the government takes a close investigatory interest. Small firms in general are likely to receive government data requests only infrequently, and are likely to not perceive a need to develop the expensive in-house skills needed to address them. Large firms will likely view their government interactions as a repeated game, with aspects reaching well beyond the question of whether to provide customer communications in cleartext. For example, by 2019, Amazon and Microsoft, two PRISM partners, had become the finalists in bidding on a ten-year, $10 billion Department of Defense cloud computing and AI program. A refusal by either firm to allow its servers to be transparent to PRISM might easily have disadvantaged Amazon or Microsoft in that bidding process.[10]

II. NATIONAL GOVERNMENT SURVEILLANCE MAY AFFECT THE NATURE OF INTERNATIONAL COMPETITION

One policy area where there is a known overlap between government surveillance practices and antitrust concerns is in the negotiations over U.S.-EU data sharing agreements, most often referred to as "Privacy Shield." We will briefly review the history of these agreements, and discuss the likely implications for competition policy.

The PRISM program, revealed in 2013 in the documents Edward Snowden brought out of the NSA, involves NSA exploitation of tech firm consumer communications on a mass scale, via the FBI's Data Intercept Technology Unit for explicit data requests, via co-optation of personnel internal to those companies, and via compromise of the encryption standards used by these firms.[11] As of 2013, PRISM was described as "the number one source of raw intelligence used for NSA analytic reports."[12]

One casualty of the PRISM revelation was what was then called the "Safe Harbor" agreement, which governed data flows between U.S.-headquartered and EU-headquartered companies. Under this agreement, U.S. companies could self-certify that they provided substantially equivalent privacy protections to their customers as EU companies provided to their customers. However, PRISM showed that U.S. tech companies were vulnerable to massive and systemic data exfiltration by the U.S. intelligence community.

An Austrian citizen, Max Schrems, brought suit in Ireland, arguing that this process of self-certification was now revealed to have been based on a lie, and that EU citizens could no longer rely on U.S. firms' self-certifications that those firms were protecting their rights. In 2015, the

8 See Tanfani, J., "Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds," March 27, 2018, Los Angeles Times. Available at https://www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html, accessed December 8, 2022.

9 See Campbell, J., A. Goldfarb, and C. Tucker (2015). Privacy regulation and market structure. Journal of Economics & Management Strategy 24(1), 47–73.

10 For the lengthy litigation history around this highly controversial contract, see Soper, T., "Pentagon cancels $10 billion JEDI cloud contract after long feud between Amazon and Microsoft," July 6, 2021, *Geekwire*, available at https://www.geekwire.com/2021/pentagon-cancels-10-billion-jedi-cloud-contract-long-feud-amazon-microsoft/, accessed December 12, 2022.

11 See Appelbaum, J. R. (2022). Communication in a world of pervasive surveillance: Sources and methods: Counterstrategies against pervasive surveillance architecture. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mathematics and Computer Science]. Eindhoven University of Technology, pp. 72-84.

12 See Madrigal, A., "Bombshell Report: NSA and FBI 'Tapping Directly' Into Tech Companies' Servers:
Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, and Apple are all implicated." The Atlantic, June 6, 2013. Available at https://www.theatlantic.com/technology/archive/2013/06/bombshell-report-nsa-and-fbi-tapping-directly-into-tech-companies-servers/276633/, accessed December 7, 2022.

Court of Justice of the European Union agreed, and invalidated the Safe Harbor agreement.[13] U.S. and EU diplomats scrambled to replace it with the "Privacy Shield" agreement,[14] which the CJEU proceeded to invalidate in its turn.[15] The newest agreement, "Privacy Shield 2.0," was agreed in 2022; President Biden has issued an executive order implementing it,[16] but the text will not come into effect till 2023. That text is also likely to be litigated, and is unlikely to survive court review, because it does not appear to meet the CJEU's standards for providing meaningful redress to EU citizens whose privacy is invaded by these surveillance systems.[17]

The implications for competition policy are substantial. If U.S. tech firms appear as a result of U.S. government surveillance to no longer be trustworthy custodians of their citizens' data, one natural response of EU authorities will be efforts to promote data localization within the EU, up to and possibly including compelling U.S. tech firms to hive off separate firms to handle EU nationals' data under different firms.

In turn, speculatively, though the EU-based firms would then be under a legal obligation to follow CJEU requirements for data privacy, national governments within the EU might be more eager to pursue a "national champions" model to encourage locally owned competition to those U.S. firms, such as French-owned search engine competitors Qwant and Algolia, and to then form close collaborative relationships with these more domestically controllable firms. Of course, there is nothing that restricts these concerns to U.S. government surveillance in particular; the U.S. has just banned Chinese telecommunications products from Huawei, ZTE, Hytera Communications, Hikvision, and Dahua,[18] showcasing the same anxiety about dealing from afar with firms that are perceived as being trusted partners of their home country's intelligence services.

III. GOVERNMENT SURVEILLANCE POLICIES FAVOR INCUMBENTS DUE TO THE COSTS THEY IMPOSE

Most models of privacy and competition focus on how the costs that regulatory compliance imposes shapes competitive structures.[19] In general, the theoretical and empirical evidence in this research that shows consumer-focused privacy regulation leads to more contraction and deters entry. The mechanism that is usually documented is that firms have to manage data flows on a customer-level explicitly. This leads to fixed costs that are better borne by large firms. However, the same mechanism is also possible when it comes to regulation that is designed to enhance government surveillance of customer data.

"Know Your Customer" regulations were developed to inhibit money-laundering and other criminal activity. However, by emphasizing face-to-face contact and verification, they also operate to discourage privacy-enhancing financial innovations, and to safeguard the business model of existing, brick-and-mortar banks. In that sense, the substantial work being done on how to update KYC regulations should take into account the potential anti-competitive impacts of the current U.S. model.[20]

13 See *Maximilian Schrems v. Data Protection Commissioner* ("Schrems I"), ECLI:EU:C:2015:650, October 6, 2015, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=16990, accessed December 12, 2022.

14 See https://www.politico.eu/wp-content/uploads/2016/06/Privacy-shield-text-for-opinion-and-annexes.pdf, July 12, 2016, accessed December 12, 2022.

15 See *Maximilian Schrems v. Facebook Ireland Limited* ("Schrems II"), ECLI:EU:C:2020:559, July 16, 2020, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=16990, accessed December 12, 2022.

16 See "Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities," October 7, 2022, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/, accessed December 12, 2022.

17 See CMS Germany, "US adopts Executive Order to implement EU-US Data Privacy Framework," November 10, 2022, available at https://www.lexology.com/library/detail.aspx?g=211ffdc2-0d59-4ef8-9516-7310fa85ff9e, accessed December 7, 2022.

18 See Woolacott, E., "U.S. Bans Chinese Telecom Kit Over National Security Concerns," available at https://www.forbes.com/sites/emmawoollacott/2022/11/28/us-bans-chinese-telecom-kit-over-national-security-concerns/, accessed December 12, 2022.

19 Campbell J, Goldfarb A, Tucker C. Privacy regulation and market structure. Journal of Economics & Management Strategy. 2015 Mar;24(1):47-73. And Johnson G, Shriver S, Goldberg S. Privacy & market concentration: Intended & unintended consequences of the GDPR. Available at SSRN 3477686. 2022.

20 The literature here is extensive, but see, for example, Chorzempa, M., *"The Cashless Revolution: China's Reinvention of Money and the End of America's Domination of Finance and Technology,"* 2021.

IV. GOVERNMENT SURVEILLANCE PROGRAMS MAY AFFECT STANDARDS AND IN TURN COMPETITION

Conventional DOJ antitrust investigations have often focused on the standards-setting process in different industries, watching for situations where one company unfairly skews the standards-setting process to favor its own products and block its competitors'. With respect to government surveillance and encryption standards, the risk is fundamentally the same, with the difference that the standards-setting process may be skewed so as to permit unfair government access to citizens' data by a government intelligence agency. NSA's actions to "enable" national and international cryptographic standards are included under a program codenamed "BULLRUN."

This sabotage has included the explicit weakening of the DES cryptographic standard issued by NIST, with the collusion of IBM; the bribery of security industry pioneer RSA to include NSA-enabled cryptographic standards; NSA influence over the ISO/IEC standardization process; and presumably other as yet undisclosed actions through to the present.[21] Each of these interventions necessarily privileges some firms in the market over others, and in turn binds those firms in closer cooperation with the intelligence community, while depriving other, less favored firms of access to revenue from government sources.

V. IS ANY OF THIS AN ANTITRUST ISSUE?

Both the FTC and competition authorities in other countries have begun to consider privacy as a component of their competitive analysis for mergers. The EU, for example when examining the Microsoft/LinkedIn merger, described privacy in personal social networks as "an important parameter of competition."[22] The government's Horizontal Merger Guidelines explicitly allow competition authorities to consider "non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation."[23] However, it is problematic if the antitrust enforcement arm is part of a governmental entity that encourages firms to share data about citizens for surveillance purposes, and argues against strong encryption. We have seen little evidence that firms' sharing of data with governments, as opposed to data privacy practices in general, are becoming part of antitrust analysis, however.

There is reason for concern that current trends in government surveillance and information management may lead to anti-competitive outcomes, even if this concern fits poorly under the existing framework of U.S. antitrust law. We have presented historic examples that suggest that government surveillance programs may give governments incentives to work with large established incumbents. However, it is not within the scope of this article to analyze those incentives empirically, and we encourage further work in this area.

---

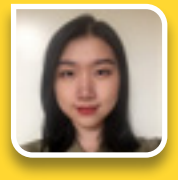
21 See Ashur, T., Luykx, A. (2021). "An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families" in Avoine, G., Hernandez-Castro, J. (eds) Security of Ubiquitous Computing Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-10591-4_4; Menn, J., "Exclusive: NSA infiltrated RSA security more deeply than thought - study," March 31, 2014, Reuters, available at https://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331, accessed December 8, 2022; and Appelbaum, J. R. (2022). Communication in a world of pervasive surveillance: Sources and methods: Counterstrategies against pervasive surveillance architecture. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mathematics and Computer Science]. Eindhoven University of Technology, pp. 72-84.

22 See Cooper, James C., Antitrust & Privacy (November 11, 2020). The Global Antitrust Institute Report on the Digital Economy 32, available at SSRN: https://ssrn.com/abstract=3733752 or http://dx.doi.org/10.2139/ssrn.3733752.

23 See Department of Justice & Federal Trade Commission, Horizontal Merger Guidelines (2010).

POPULAR MOBILE APPS IN THE PANDEMIC ERA: A GLIMPSE AT PRIVACY AND COMPETITION

BY GINGER ZHE JIN, ZIQIAO LIU & LIAD WAGMAN[1]


1 Ginger Jin is a professor of Economics at the University of Maryland & NBER, Email: ginger@umd.edu. Ziqiao Liu is a graduate student of Economics at the University of Maryland, Email: zliu26@umd.edu. Liad Wagman is a professor of Economics at Illinois Institute of Technology, Email: lwagman@stuart.iit.edu. We are thankful to Apptopia and the Data Catalyst Institute for providing access to the data.

I. INTRODUCTION

According to App Annie (2022), global downloads of mobile apps has reached 230 billion in 2021, and an average user in the top 10 markets spent more than 4 hours and 48 minutes on mobile in 2021, up 30 percent from 2019. Publishers, meanwhile, released 2 million new apps in 2021, 77 percent of which were on Google Play. Consistently, global mobile ad spend reached $295 billion in 2021, a 23 percent increase from 2020.

There is no doubt that social distancing, travel limits, and other pandemic-related policies have contributed to these changes. Even more impressively, these changes happened as consumers' concerns over privacy potentially grew, with many governments having adopted or in the midst of considering the adoption of new privacy and data regulations. Given the role of mobile apps in digital economy, it is important to understand how the demand and supply of mobile apps evolve in this dynamic environment, and how the evolution differs in markets with different privacy and data regulations.

Since the European Union (EU) rolled out its landmark General Data Protection Regulation ("GDPR") in May 2018, policymakers have either adopted or have been considering adopting similar regulations around the globe. That includes the U.S., where although a comprehensive federal law on data and privacy remains elusive, California implemented the California Consumer Privacy Act ("CCPA") in January 2020 and is on the way to roll out the supplemental California Privacy Rights Act ("CPRA") in July 2023. Virginia and Colorado enacted similar laws, effective January 1, 2023 and July 1, 2023, respectively.

Despite these efforts, the regulatory environment is still quite different between the U.S. and the EU. The GDPR defines consent as "freely given, specific, informed and unambiguous" given by a "clear affirmative action." In short, aside from cases of legitimate interest or other contractual clauses, the GDPR requires consent to be opt-in. CCPA, in contrast, allows firms to set data collection and data sharing as the default, as long as consumers can opt out for alternative settings. This opt-out approach entails less consumer awareness and less consumer action than opt-in. Furthermore, GDPR applies to any data collectors that offer goods and services to individuals in the EU, whereas CCPA is only applicable to for-profit data collectors that conduct business in California, have annual gross revenue above 25 million dollars, involve more than 50,000 data subjects, or derive more than 50 percent of their revenue from selling personal information. Such qualified applicability can shield many small and medium-sized mobile app developers from CCPA, and leave room to avoid or mitigate the potential impact of CCPA on app developers. In light of these regulatory differences, we compare app performance in the U.S. and five major European countries (UK, France, Germany, Spain and Italy, referred to as "EU5").

It is worth noting that the U.S.-EU5 comparison may capture many differences between the U.S. and the EU. Aside from the regulatory differences, the U.S. is significantly larger than any individual European member state, and U.S. and EU consumers may differ in smartphone penetration, privacy awareness, user habits, language, demographics, etc. Even if the regulatory difference is the most important dimension to consider, it is unclear how a more comprehensive and more stringent data regulation like GDPR would affect app developers and app users once the pandemic environment drives up the time users spend on smartphones.

For instance, to the extent that privacy and data regulations may raise barriers to entry (in terms of compliance costs and consumer willingness to try new apps), one may expect new apps to face more difficulties entering and growing in a market with stricter regulations. App developers may target a less regulated market first before meeting more stringent regulations in other markets. However, a large expansion in demand may increase the prospects of total revenue, even if it is difficult to attract and monetize each potential consumer.

Consumers may be more willing to accept a reduction in privacy when they anticipate more benefits from mobile apps than alternative uses of time. This would encourage new apps to enter and grow regardless of the regulatory strictness. Conversely, more digital experience may prompt consumer attention to privacy and data concerns, especially if the regulation brings these issues to the surface via opt-in consent windows. Consumers may even feel safer under a stronger privacy and data regulation, and have more comfort downloading and using new apps. Besides these offsetting factors, an expansion in demand may intensify competition between new, young and established apps, and the nature of the competition may depend on the strength of privacy and the regulatory environment.

In fact, the literature has painted a mixed picture regarding the impact of the GDPR before and after 2018 (mostly before the pandemic). On the one hand, studies show that the GDPR has reduced venture investment in technology startups based in the EU,[2] reduced web traffic,

2 Jian Jia et al. *The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment*, MARK. SCI., 40, no. 4 (2021): 661–84. https://doi.org/10.1287/mksc.2020.1271.

e-commerce revenue and persistent cookies in Europe,[3] increased market concentration among web technology vendors[4] raised the search costs of GDPR-covered users,[5] and reduced consumer surplus from mobile apps because more apps exit and fewer enter post the GDPR.[6] These studies suggest that EU countries may suffer from less entry, less innovation, and less market competition because of the GDPR.

On the other hand, some studies find the GDPR to have zero or offsetting effects. For example, Zhuo et al. find that the GDPR has had no effect on interconnection agreements between EU and out-of-EU network providers.[7] Aridor et al. show that, although the opt-in requirement of the GDPR reduced the number of identifiable consumers, an online travel intermediary is able to better track remaining consumers and increase their average advertising value. Following 900+ news and media websites in the U.S. and EU, Lefrere et al. find that, despite an initial reduction, visitor tracking among EU websites bounced back after a few months, and GDPR has no significant effect on EU websites' traffic rankings, new content provision, or social media engagement with new content.[8] They also find no difference in the monetizing strategy or survival rate of content providers across the EU and the U.S. These findings suggest that the initial, negative effects of the GDPR may not harm the survival and development of online innovations.

As detailed below, the post-pandemic increase in mobile app usage is large and persistent. This demand shock provides an excellent test bed to study the supply of new apps and their competition with established apps. In light of regulatory and other differences between the U.S. and the EU, we compare the U.S. with EU5 before and after the onset of the COVID-19 pandemic.

We also compare six app categories that are arguably more sensitive to user privacy (Games, Health & Fitness, Social, Communication, Shopping, and Finance) with all other categories (Tools, Weather, News & Magazines, etc.); we refer to the two groups as "privacy-sensitive" and "all other" categories, respectively. Strictly speaking, apps tend to involve some type of data transmission in and out of a user's smartphone – apps may utilize location information, a phone's IP address is embedded in signal transmission protocols, and even a user's app use time, session lengths and keystrokes could be correlated with some user attributes, even if such information is not always personally identifiable.

We single out the six privacy-sensitive categories because they are likely to involve the transmittal and potential collection of additional or more sensitive personal information, such an individual's contacts, shopping history, health, finances, and aspects related to cognition. For example, shopping and finance apps have traditionally been associated with price discrimination in the economics of privacy literature and often require a user's address and other personal information;[9] health and fitness may capture biometric information in addition to location and movement changes; and gaming, social and communication apps often involve interactions with other users on the same app. While we believe these six categories may be more privacy-sensitive than all other categories as a whole, we also note that the two groups may differ in other dimensions; for instance, users may derive more benefits from an app if they can interact with each other in real time, or users may care more about timely information from health, fitness and financial apps even if these apps require them to give away location, biometric, and other personal information. Thus, privacy is not the only factor contributing to the observed differences between privacy-sensitive and all other categories.

In short, our descriptive comparison – U.S. vs. EU5, privacy-sensitive vs. all other categories – reflect changes before and after the onset of the pandemic in the data. These changes could be driven by regulatory, privacy, and other fundamental differences across countries and categories. Since the mechanisms behind these changes are manifold, readers should not interpret our summary statistics as causal effects of any particular factor or any particular mechanism. Rather, we hope the data patterns presented in this paper can motivate more and deeper research in this area.

---

3 Samuel Goldberg et al. *Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes*, (2021).
Timothy Libert et al. *Changes in Third-Party Content on European News Websites after GDPR*, Factsheet. REUTERS INSTITUTE (2018). Adrian Dabrowski et al. *Measuring Cookies and Web Privacy in a Post-GDPR World*, INTERNATIONAL CONFERENCE ON PASSIVE AND ACTIVE NETWORK MEASUREMENT. Springer, 258–270 (2019). Raffaele Congiu et al. *The Impact of Privacy Regulation on Web Traffic: Evidence From the GDPR*, (2022). Guy Aridor et al. *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*. NBER Working Paper, w26900, (2020).

4 Garrett Johnson & Scott Shriver. *Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR*, (2019). Christian Peukert et al. *Regulatory spillovers and data governance: Evidence from the GDPR*, MARK. SCI., (2022).

5 Yu Zhao et al. *Privacy Regulations and Online Search Friction: Evidence from GDPR*, NBER workshop on the Economics of Privacy, (2022).

6 Rebecca Janßen et al. *GDPR and the Lost Generation of Innovative Apps*, NBER Working Paper, w30028 (2022).

7 Ran Zhuo et al. *The Impact of the General Data Protection Regulation on Internet Interconnection*, TELECOMM POLICY, 45(2), (2021).

8 Vincent Lefrere et al. *Does Privacy Regulation Harm Content Providers? A Longitudinal Analysis of the Impact of the GDPR*, (2022).

9 Vincent Conitzer et al. *Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases*, MARK. SCI., 31(2), 277-292 (2012). Jin-Hyuk Kim & Liad Wagman. *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, RAND J ECON, 46(1), 1-22, (2015). Alessandro Acquisti et al. *The Economics of Privacy*, JEL, 54(2), 442-492, (2016).

We find that in the categories of Games, Health & Fitness, Social, Communication, Shopping, and Finance, the U.S. is "friendlier" than EU5 to new apps released after January 2020. In particular, relative to EU5, apps in the U.S. have a greater chance to be ranked in a top 200 list in the first two months of app age, a greater chance to stay as a top 200 app in the third, fourth and fifth months since the first time making top 200, and a greater share of daily active usage within top 200 apps. Interestingly, this advantage subsequently dissipates as the U.S. and EU5 converge; and the advantage is negligible in all other app categories.

To explain the temporary U.S. advantage for new apps in the six privacy-sensitive categories, we can think of many potential reasons: for example, a preference among developers to target or first launch in the U.S., more lax and more fragmented data regulations in the U.S., or U.S. users' stronger willingness to try new apps. Further research is needed to distinguish these potential explanations.

We further find that in both the U.S. and EU5, and across all categories, top 200 apps that were released on or after March 2020 are significantly more ad-based than top 200 apps that were released by January 2020, suggesting that the role of ad revenue in app success (in terms of making top 200) has increased post March 2020, possibly because users are more tolerant of ads as they spend more time on mobile apps.

II. DATA AND GLOBAL TRENDS

Our data comes from Apptopia, a third-party data intelligence company that tracks mobile apps on the iOS and Google Play stores, tracking mobile apps through June 1, 2021.

The first part of the data records all mobile apps that have been ever been released, including app id, app name, app creation time, app developer id, app description, and app categories. While this cross-sectional metadata covers the universe of mobile apps up to June 1, 2021, it does not specify whether and how a mobile app targets users in a specific country. In theory, a mobile app released on iOS or Google Play could be available anywhere as long as the user's smartphone can access the app store. In this sense, the metadata can only measure the time of an app's global entry.

The second part of the data tracks high performance apps. Once an app appears on a top-ranking list of iOS or Google Play, Apptopia tracks its downloads, # of monthly active users, # of daily active users, and app star ratings by the user's country and app store, until the app's downloads drop to zero for at least six months. If an app is tracked, Apptopia also estimates the app's download revenue, ad revenue, and in-app purchase revenue by user country and app store. This allows us to define whether an app has any ad revenue at all and whether an app is "ad-based" when at least 50 percent of its revenue comes from ads.

In this article, we focus on Google Play only because the vast majority of new apps released after January 2018 were released on Google Play (81.06 percent according to our calculation from the Apptopia metadata),[10] and Google Play has outgrown iOS since 2014 in terms of the cumulative number of apps released (App Annie, 2022). Another reason to focus on Google Play is that Apple adopted a few new privacy policies in April 2021 and October 2021, which are either near or after the end of our sample period (June 2021). In comparison, Google Play has not changed its privacy policies significantly (although Google announced potential changes in the future in response to Apple's changes). Finally, Google Play used to provide a top 500 ranking list per app category, but shortened it to top 200 in September 2019. To be consistent, we focus on top 200 only throughout our sample period (January 1, 2018 to June 1, 2021). Our top 200 analyses focus on a comparison between the six privacy-sensitive categories and all other categories. Each category has its own top 200 list per country-month. Apps are also separately tracked in top 200 lists by whether they are free-to-install or are pay-to-install.

Based on the metadata, the left graph of Figure 1 plots the number of new apps released on Google Play per month, with the dark grey area for free apps, and the black area for pay-to-install (paid) apps. Throughout the sample period, the vast majority of new apps are free. The vertical light grey bar denotes the onset of the pandemic (January to March 2020). We choose a band of time rather than a specific date, because China locked down Wuhan on January 23, 2020, airlines and countries began to impose travel restrictions in February 2020, the U.S. declared a national emergency on March 13, 2020, and the EU began to restrict all non-essential travel from other countries into the EU on March 17, 2020. Obviously, app entries on Google Play were declining before the onset of the pandemic, but this trend was reverted in early 2020. More specifically, the number of new apps began to increase in January 2020, and peaked in May 2020 before declining again. Unsurprisingly, the entry spike is driven by free apps.

10 Our count of Google Play apps includes those that were released on both iOS and Google Play and those released on Google Play only.

The right graph of Figure 1 plots the total count of monthly active users of top 200 apps on Google Play, for the U.S. and EU5 separately, across all categories. As our data is aggregate without individual user id, a user who is active on two top 200 apps is counted as two users. Consistent with the industry trends reported by App Annie (2022), app usage increased over time and the pattern is remarkably similar between the U.S. and EU5. The huge increase in monthly active users in mid 2019 is largely due to an increase in specific categories like Social and Communication, and the ups and downs between January and May 2020 mainly result from changes in the Game category, which is the single largest category on Google Play. In contrast to the short-lived spike of app entry in May 2020, we observe a rapid increase of monthly active users in June 2020, and this increase is persistent throughout the end of the sample period (June 2021), even after the U.S. and EU5 gradually loosened social distancing policies and travel limits.

In short, Figure 1 suggests that a spike of app entries has coincided with a persistent usage growth for popular mobile apps after the onset of the pandemic.

Table 1 presents a basic comparison between the U.S. and EU5 for top 200 apps in the six privacy-sensitive and all other categories from May 2019 to June 2021. To simplify the comparison, we report EU5 numbers as average per country. Because each category, month and user country has its own top 200 list on Google Play (for free and paid apps separately), the number of unique top 200 apps per month is more than 16000 in the U.S. and more than 13000 per country in EU5. In both columns, new apps released after January 2020 account for a small but non-trivial fraction of top 200 apps. This fraction alone suggests that slightly more new apps made top 200 in EU5 than in the U.S. in the privacy-sensitive categories (14.7 percent vs. 13.6 percent), but fewer new apps made top 200 in EU5 in all other categories (8.7 percent vs. 13 percent). Because this fraction is computed by the count of unique apps, it could be driven by the ease/difficulty of new apps making top 200 or their turnover in and out of top 200. Later on, we explore the likelihood of becoming and remaining a top 200 app.

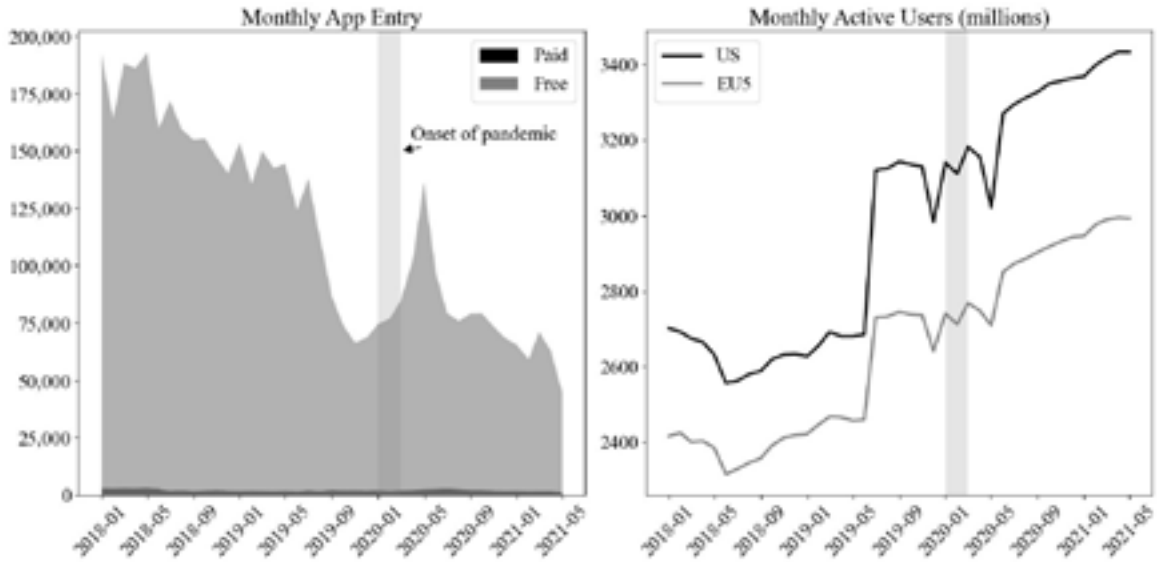


Figure 1: Global App Entry based on metadata and Total Monthly Active Users based on Top 200 apps (Google Play Store)

Within the six privacy-sensitive categories, 57.4 percent of top 200 apps in the U.S. have any ad revenue, which is lower than in EU5 (70.8 percent). Consistently, the fraction of ad-based top 200 apps is lower in the U.S. than in EU5 (33.9 percent vs. 43.1 percent). As for app age, top 200 apps in the U.S. are almost 100 days older than those in EU5. Similarly, for top 200 apps in all other categories, those in the U.S. are less likely to have any ad revenue, less likely to be ad-based, are older, and are of higher star ratings than those in EU5. A comparison between privacy-sensitive and all other categories suggests that top 200 apps in all other categories are less reliant on ad revenue, and are on average younger and have slightly lower ratings than those in privacy-sensitive categories.

Table 1: Summary Statistics of Top 200 apps on Google Play, 2019-05-01 to 2021-06-01

Variable (per month)	U.S.	EU5 (avg. per country)
# of unique apps	15,711	12,781
Privacy-sensitive categories		
# of unique apps in privacy categories	1,804	1,537
# (%) of unique privacy apps released after 1/2020	246 (13.6%)	226 (14.7%)
% of privacy apps with any ad revenue	57.4%	70.8%
% of privacy apps that are ad-based	33.9%	43.1%
avg age of privacy apps (days)	1,297	1,201
avg star rating of privacy apps	4.18	4.13
All other categories		
# of unique apps in all other categories	14,398	11,735
# (%) of unique all other apps released after 1/2020	1,882 (13.0%)	1,104 (8.7%)
% of all other apps with any ad revenue	32.6%	39.5%
% of all other apps that are ad-based	26.9%	32.6%
avg age of all other apps (days)	1,152	1,072
avg star rating of all other apps	4.15	4.11

Notes: Data source: Apptopia data on the performance of top 200 apps in the Google Play Store. Every variable is a monthly average including free and paid apps.

III. GROWTH AND SURVIVAL OF NEW APPS

While the onset of the pandemic provides an opportunity for new apps, it is an open question as to how they perform after entry, and whether this performance depends on the user's country and the privacy sensitivity of the app's primary category.

Generally speaking, mobile apps face intensive competition: every month, 50k to 200k new apps have entered the global Google Play store, but consumers are unlikely to go beyond the first few pages of the top-ranking lists if they conduct a general search for mobile apps. Figure 2 shows the probability of an app first showing up in a top 200 list as a function of the app's age. For privacy-sensitive and all other categories (separately), Figure 2 plots the probability of reaching a top 200 ranking by user geography (U.S. vs. EU5) and app release time (by January 2020 versus on and after March 2020).[11]

Figure 2 suggests that the likelihood of reaching a top 200 ranking is highest in the first month of app's release. Even before the pandemic, it was relatively easier for a brand new app to make top 200 in the U.S. than in EU5, and this difference quickly dissipated after the app's first month of age. This pattern held in both privacy-sensitive and all other categories.

For apps released by January 2020 (as compared to those released since March 2020), the first month difference between the U.S. and EU5 is magnified for both privacy-sensitive and all other categories, and the difference remains positive for the second month of app age.

11 We drop apps that entered Google Play Store in February 2020 given variations of pandemic status and limits in that month.

In privacy-sensitive categories, EU5 catches up with the U.S. for apps in the third, fourth and sixth-months of age, but these differences do not completely offset the U.S.-EU5 differences in the first two months. After the seventh month of age, the chance of an app making top 200 converges to the pattern of apps released before January 2020. The convergence in all other categories is even faster.

Figure 3 plots the extent to which a top 200 app remains on the list once it first appears as top 200. By definition, every top 200 app is on the list in the first month of making the list. However, the chance of staying on the list is slim and drops sharply right after: for the apps that were released by January 2020 and have made top 200 at some point, only 5-6 percent of them remain on the list in the second month, 2-3 percent remain in the third month, and less than 2 percent stay on the list after the fourth month. While this pattern is similar for the U.S. and EU5, the chance of survival is relatively higher in the U.S. For apps that were released since March 2020, the chance of survival improves slightly, especially for apps in the privacy-sensitive categories, that are offered in the U.S., and in their third-, fourth- and fifth-months since the apps first made top 200.

Figure 2: Probability of New Apps Entering Top 200 on Google Play

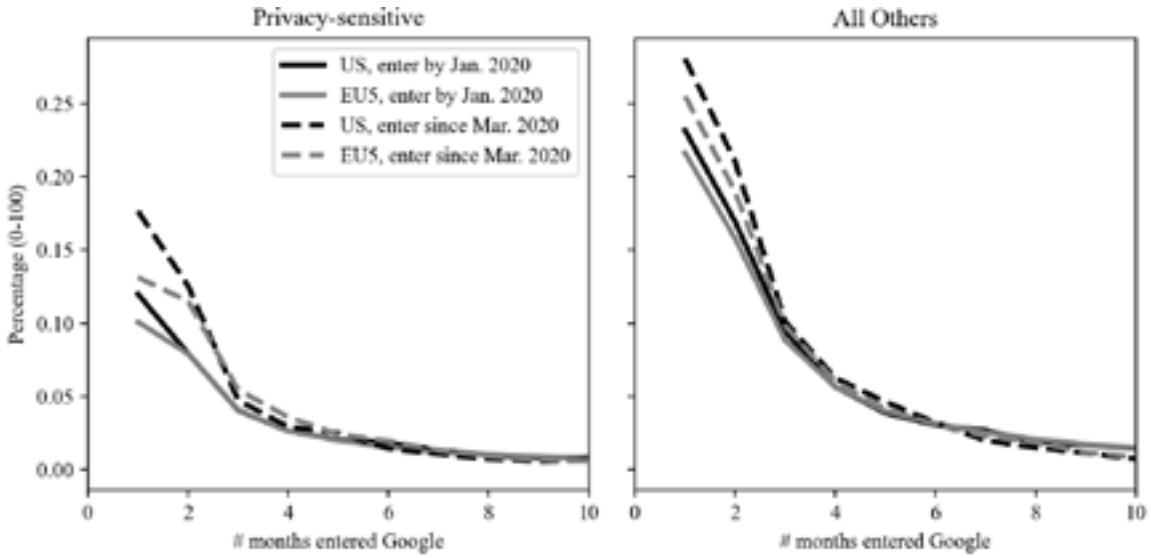
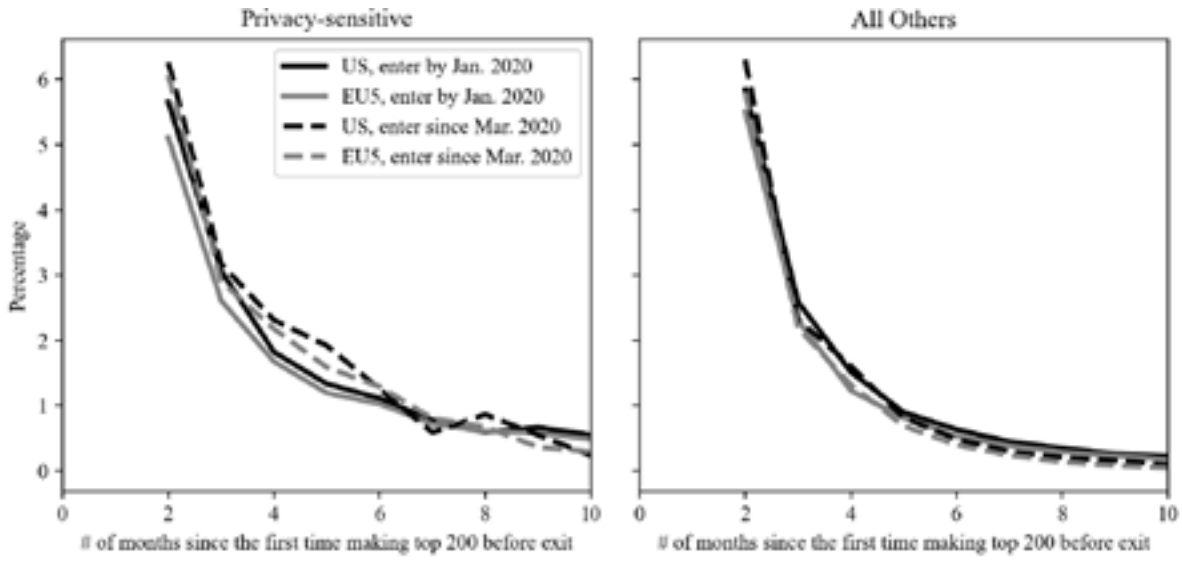


Figure 3: Survival Rate of New Apps Entering Top 200 on Google Play

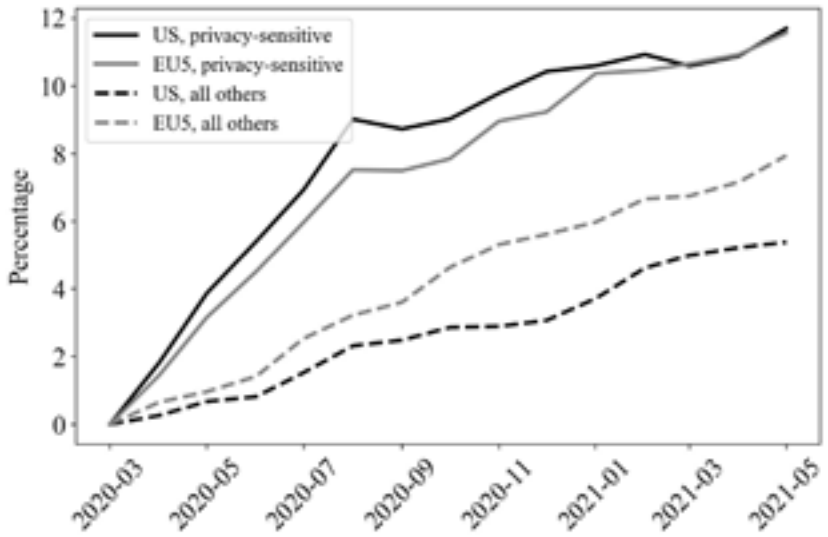


The entry and exit of top 200 apps, while informative, does not provide information regarding how a top 200 app performs relative to other ranked apps. To address this, we compute the percentage of top 200 apps' daily active usage that originates in apps released by January 2020. By definition, this percent increases over time, as more new apps entered Google Play after January 2020 and more of them make top 200 over time. Figure 4 shows that, in privacy-sensitive categories, new apps released post March 2020 have accounted for roughly 9 percent

of top 200 daily active usage in the U.S. since August 2020. This is more than 1 percentage point higher than that of EU5 until the end of 2020. In contrast, in all other categories, only 2-4 percent of top 200 daily active usage in the U.S. are driven by new apps released post March 2020, and these percentages are persistently below that of EU5.

Altogether, Figures 2, 3 and 4 suggest that, in the privacy-sensitive categories, there are more breakthrough new apps in the U.S. than in EU5 after the onset of the pandemic, in terms of a greater chance to make top 200 in the first two months of app age, a greater chance to stay on top 200 in the third, fourth and fifth months since the first time making top 200, and a greater share of daily active usage within top 200 apps. This advantage is less prominent in all other categories, if it exists at all. The U.S. vs. EU5 advantage in the privacy-sensitive categories is also temporary, as the U.S. and EU5 converge on the share of daily active usage by new apps in the last three months of our data (March to May 2021).

Figure 4: % Daily Active Usage of Apps Released Since March 2020 Among Top 200

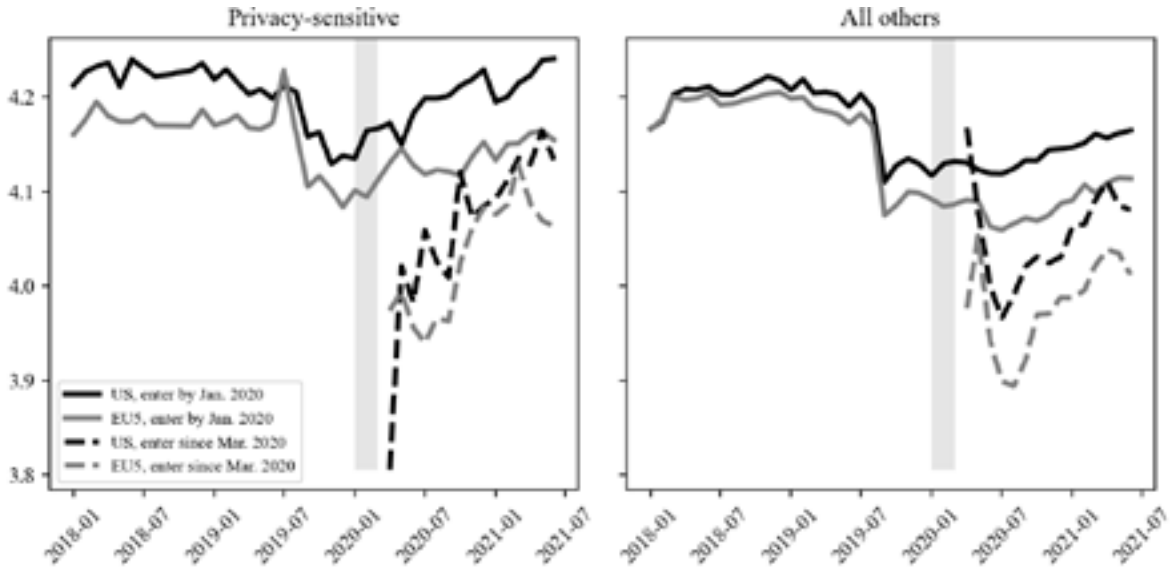


IV. AD RELIANCE AND QUALITY RATINGS OF NEW APPS

While the U.S. appears friendlier than EU5 to new apps in privacy-sensitive categories, one may wonder whether this friendliness may foster more ad-reliant and/or lower quality apps in the U.S. If so, more ad-reliance and lower quality could undermine user benefits from new apps. At the same time, advertising is an important source of revenue for mobile apps, especially free-to-install apps. A market more tolerant of ad-based apps could provide more financial incentives for app developers to innovate and improve app quality, as Shiller, Waldfogel and Ryan (2018) have shown in the context of ad blockers reducing the traffic and quality of websites.

Figure 5 plots the percentage of top 200 apps that are ad-based, conditional on having any positive revenue (from installing, advertising, in-app purchase, etc). As in Figures 2 and 3, Figure 5 plots a graph for privacy-sensitive and all other categories separately. Each graph has a separate line for the U.S. and EU5, as well as by apps released by January 2020 versus apps released since March 2020.

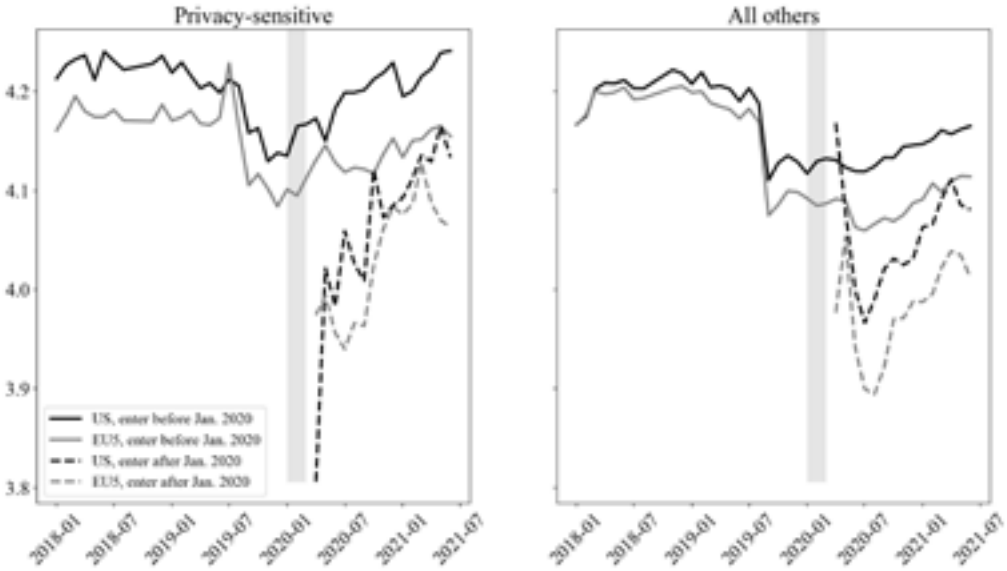
Figure 5: Percentage of Ad-Based Top 200 Apps



Consistent with Table 1, top 200 apps in EU5 are more likely to be ad-based across the sample period and in all categories. For apps released by January 2020, the U.S.-EU5 gap expands after the onset of the pandemic in both privacy-sensitive and all other categories. However, for apps released on or after March 2020, top 200 apps in the U.S. are catching up with their EU5 counterparts in the privacy-sensitive categories, but not in all other categories. These mixed patterns suggest that the U.S. market is friendlier than EU5 for new ad-based apps in privacy-sensitive categories. Interestingly, in both the U.S. and EU5 and across all categories, top 200 apps that were released post March 2020 are significantly more ad-based than top 200 apps that were released before January 2020. This suggests that the role of ad revenue in app success (in terms of making top 200) has increased post March 2020, probably because users are more tolerant of ads as they spend more time on mobile apps.

Figure 6 follows the same structure as Figure 5, but presents the average star ratings of top 200 apps in the U.S. and EU5 — based on whether the apps were released by January 2020 or since March 2020, in privacy-sensitive and all other categories separately. For top 200 apps released by January 2020, there was a big drop in August-September 2019 because Google changed its algorithm for determining an average star rating, which applies to both the U.S. and EU5. Regardless of this technical change, the U.S. top 200 apps demonstrate higher average ratings than those in EU5, and this gap expands soon after the onset of the pandemic, especially post June 2020 for privacy-sensitive categories, and post April 2020 for all other categories. This suggests that the pandemic-driven usage expansion in top 200 apps may help old high-quality apps to stand out more in the U.S., probably because the U.S. market is much larger than each individual member state in EU5.

Figure 6: Average Ratings of Top 200 Apps



For top 200 apps released on or after March 2020, their average ratings are consistently lower than that of older apps. This is understandable, given their relatively younger age and shorter time period for improving upon market feedback. For the new apps in all other categories, we still observe a rating premium between the U.S. and EU5, similar to the gap for the apps released by January 2020. But for the privacy-sensitive categories, the new top 200 apps in EU5 began to catch up with the U.S. in October 2020, which almost closed the U.S.-EU5 gap before the gap expanded again in March 2021. This temporary catch-up is intriguing, and is most likely driven by the fact that, during this time period, young U.S. apps that were released on or after March 2020 and dropped out of top 200 have ratings similar to young apps that entered top 200 each month. This keeps the average ratings of top 200 U.S. apps relatively flat compared to the EU5, where young apps dropping out of top 200 have lower ratings on average than young apps entering the same month.

V. CONCLUSION

We offer a descriptive comparison between the U.S. and EU5, contrasting apps in a group of more privacy-sensitive categories against apps in all other categories, and changes before and after the onset of the COVID-19 pandemic.

Globally, we observe a spike of new app entries in May 2020 while the monthly active users of top 200 apps grow steadily soon after the onset of the pandemic. This suggests that app entry and market expansion go hand in hand. In all categories, we find that apps released on or after March 2020 had a better chance to become top 200 in the first few months of app age than apps released by January 2020, suggesting that market expansion is helpful for the development and growth of new apps.

In the app categories of Games, Health & Fitness, Social, Communication, Shopping, and Finance, we find the U.S. is “friendlier” than EU5 to new apps released on or after March 2020. Apps in the U.S. have a greater chance to be ranked in a top 200 list in the first two months of app age, a greater chance to stay as a top 200 app in months 3 through 5 since their first time making top 200, and a greater share of daily active usage within top 200 apps. This advantage subsequently dissipates and is generally negligible in all other app categories.

We further find that in both the U.S. and EU5, and across all categories, top 200 apps that were released post March 2020 are significantly more ad-based than top 200 apps that were released by January 2020, suggesting that the role of ad revenue in app success (in terms of making top 200) has increased post March 2020, possibly because users are more tolerant of ads as they spend more time on mobile apps.

These changes, especially the temporary advantage of the U.S. for new breakthrough apps in the six privacy-sensitive categories, are subject to multiple explanations. For example, some app developers may prefer to target the U.S. market only or to launch new apps in the U.S. first, which could be related to a more active venture capital market in the U.S., or more lax and more fragmented data regulations in the U.S. It is also possible that U.S. users are less aware or less concerned of privacy and data issues. Alternatively, U.S. users may have a stronger willingness to try new apps, despite holding similar privacy concerns as EU citizens. Different market sizes, different demographics, and different user preferences for social, shopping, health and fitness apps could also contribute to the observed U.S.-EU5 differences. Since the mechanisms behind these differences are manifold, readers should not interpret our findings as causal effects. Identifying the underlying mechanisms merits further research.

PRIVACY PROTECTIONS THROUGH ANTITRUST ENFORCEMENT

BY DANIEL A. HANLEY & KARINA MONTOYA[1]

1 Daniel A. Hanley is a Senior Legal Analyst at the Open Markets Institute. Karina Montoya is a Reporter-Researcher with the Center for Journalism & Liberty, a program of the Open Markets Institute.

I. INTRODUCTION

In recent years, powerful technology corporations Google and Meta (the parent company of Facebook) have successfully eluded meaningful regulation by U.S. lawmakers, raising the question of what legal approach would most effectively bring them to heel.[2] Lawmakers and advocates increasingly consider privacy law and antitrust enforcement as the most potent legal avenues capable of taming Big Tech. Both areas of law are now seen as vehicles for a fundamental restructuring of the technology industry, one that would promote competition, curtail unfair practices such as self-preferencing, break up monopoly power, and provide protections to consumer privacy.

Unlike in other countries,[3] the United States does not have a general law that protects consumer privacy rights. Instead, privacy regulations exist through a patchwork of narrowly targeted and discrete laws, most of which predate the internet, and are enforced by an alphabet soup of federal and state agencies.[4]

At the national level, the Federal Trade Commission ("FTC") is the *de facto* federal privacy regulator because the agency can regulate data usage, acquisition, and user privacy through Section 5 of its originating statute, which grants it expansive authority to prohibit unfair or deceptive acts or practices as well as unfair methods of competition throughout the entire economy.[5]

Without a comprehensive privacy and data law, the predominant protections afforded to consumers over how their data is collected and used is through corporation-provided notices, which ultimately force users to agree to lengthy, non-negotiable, and near incomprehensible terms of service contracts.[6]

In the absence of comprehensive federal protection, states started to exercise their legislative powers about five years ago and enacted their own laws to protect consumer privacy. The first enacted law was California's Consumer Privacy Act ("CCPA") in 2018.[7] CCPA established several rights for Californians that give them more control of their personal data, including the right to know what information is collected and shared about them, to opt out from the sale of such data for advertising purposes, and the right to have it deleted as well. In 2020, California strengthened the CCPA by adding more requirements and created the state's first privacy protection agency, incentivizing other states to enact similar laws that will go into effect next year.[8]

Action from Congress and federal agencies have also moved forward. The American Data Privacy and Protection Act,[9] a breakthrough bipartisan bill to establish federal data privacy protections, is ready for a full House vote. Among other actions, while Congress considers legislation, the FTC has initiated a rulemaking to crack down on commercial surveillance.[10]

These recent efforts to enact privacy regulations are both admirable and necessary, but without the passage of a federal law like the American Data Privacy and Protection Act, federal enforcers see antitrust law as an essential supplement to check the power of Big Tech and create the opportunity for consumers to be provided some much-needed privacy protections. Recent examples of this effort include the Depart-

2 See Cat Zakrzewski, *Tech Companies Spent Almost $70 Million Lobbying Washington in 2021 as Congress Sought to Rein in Their Power,* Wash. Post (Jan. 21, 2022), https://www.washingtonpost.com/technology/2022/01/21/tech-lobbying-in-washington/.

3 For example, the European Union enacted the General Data Protection Regulations in 2018. See Danny Palmer, *What is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZD Net (May 17, 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

4 See generally Daniel J. Solove, *A Brief History of Information Privacy Law*, Gwu. L. Fac. Pub. & Other Works (2006), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications. For a list of the major sector specific laws governing privacy, see Stephen P. Mulligan & Chris D. Linebaugh, Cong. Research Serv., R45631, *Data Protection Law: An Overview*, 7-35 (2019).

5 15 U.S.C. § 45; Erika M. Douglas, *The New Antitrust/data Privacy Law Interface*, 130 Yale L.J. Forum 647, 651 (2021).

6 Frank Pasquale, *Privacy, Antitrust, and Power*, 20 Geo. Mason L. Rev. 1009, 1012 (2013); Maurice E. Stucke, "Should We Be Concerned About Data-Opolies?," 2 Geo. L. Tech. Rev. 275, 289 (2018); James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, U. Ill. J.L. Tech. & Pol'y, Spring 2005, at 1, 2 (describing the development and proliferation of privacy policies among internet services).

7 Cal. Civ. Code § 1798.140.

8 Id. § 1798.199.10 (establishing the California Privacy Protection Agency). For a list of other state privacy laws, see Sheila A. Millar & Tracy P. Marshall, *The State of U.S. State Privacy Laws: A Comparison*, Nat'l L. Rev. (May 24, 2022), https://www.natlawreview.com/article/state-us-state-privacy-laws-comparison.

9 *H.R.8152 - American Data Privacy and Protection Act*, Congress.gov, https://www.congress.gov/bill/117th-congress/house-bill/8152 (last visited Nov. 15, 2022).

10 Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

ment of Justice's lawsuit against Google's prolific use of restrictive agreements to maintain its dominant position in internet search, and the FTC's lawsuit challenging Meta's acquisitions of WhatsApp and Instagram.[11]

Traditional scholars have voiced significant skepticism with using antitrust to facilitate privacy protections. Their skepticism stems from at least three sources. First, scholars assert that privacy is merely a narrow situationally dependent consumer preference.[12] Second, traditional antitrust scholars assert that, under the predominant analytical framework governing antitrust law over the last four decades, antitrust has a narrow focus, which is primarily to prevent price increases to consumers and collusive behavior and, thus, should not be used to facilitate privacy protections for consumers.[13] Third, advocates have generally been unsuccessful with providing an articulable and comprehensive framework for how antitrust policy can both protect and facilitate data privacy while also facilitating robust and fair competition between firms.[14]

This Article attempts to ease the tension between antitrust law and privacy by detailing their complementary nature – the need for which has become more apparent since July 2021 when President Biden issued a sweeping executive order calling for increased market competition, in part, by prioritizing the protection and enhancement of data privacy rights and antitrust enforcement.[15]

II. DATA ACQUISITION AND PRIVACY ARE FUNDAMENTAL ASPECTS OF COMPETITION IN TECHNOLOGY MARKETS

Data and privacy are often at odds with one another: more of one typically means less of the other. Technology companies typically collect data as a byproduct of user action (e.g. a user's browsing history), but it can also be purchased from exchanges and collected from other tools that track users across the internet.[16] Privacy defines the limits on and the rules governing data collection by corporations. In many cases, due to the diverse ways services and applications are collecting and using data, privacy cannot achieve a singular goal or even be considered categorically good. For example, if a search engine was completely barred from collecting at least some, even anonymized, data from its users, it might be exceptionally difficult to increase the relevancy of search results and provide a quality product to consumers that can compete effectively.[17] In some cases, fewer privacy protections are warranted; in others, more is warranted.[18] However, when privacy is described as merely governing data collection, and when data is reduced to a benign byproduct of users' actions, this incomplete picture misses the critical nature of this key resource being bartered in technology markets.

Simply stated, data and privacy rules governing how data is collected, used, and sold are a fundamental aspect of the technology industry's competitive environment. Indeed, data is the foundational element atop which technology companies build their business operations; it is the market they operate in.[19] Without the ability to acquire as much data as possible from consumers with impunity, it is doubtful that modern internet titans such as Google and Meta would exist in their current forms. Given that many of the services provided by technology companies are free, privacy protections afforded to consumers are an essential non-price variable of product quality.

11 Amended Complaint, *United States v. Google LLC*, No. 20-03010 (D.D.C. Jan. 15, 2021); First Amended Complaint for Injunctive and Other Equitable Relief, *Fed. Trade Comm'n v. Facebook, Inc.*, No. 20-03590 (D.D.C. Aug. 19, 2021) (hereinafter "FTC Facebook Complaint").

12 See generally Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 Antitrust L.J. 121, 151-52 (2015).

13 See, e.g. Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, Antitrust Source, Dec. 2014, at 1 ("the acquisition and use of big data by online firms is not the type of conduct captured by the antitrust laws."), http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/dec14_tucker_12_16f.authcheckdam.pdf; see Lina Khan & Sandeep Vaheesan, *Market Power and Inequality: The Antitrust Counterrevolution and Its Discontents*, 11 Harv. L. & Pol'y Rev. 235, 270-71 (2017) (describing the goals and beliefs of the Chicago School of Economics that Robert Bork advocated for).

14 Allen P. Grunes, *Another Look at Privacy*, 20 Geo. Mason L. Rev. 1107, 1127 (2013); Douglas, *supra* note 5, at 658, 667.

15 Exec. Order No. 14,036, 86 Fed. Reg. 36,987 (July 14, 2021).

16 Daniel A. Hanley, *A Topology of Multisided Digital Platforms*, 19 Conn. Pub. Int. L.J. 271, 294, 303-05, 319 (2020).

17 See generally Maurice E. Stucke & Allen Grunes, *Big Data and Competition Policy*, 289 (2016) (explaining the need for data-based businesses to obtain minimum efficient scale to be viable competitors).

18 Daniel J. Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087, 1090 (2002); Pasquale, *supra* note 6, at 1016-17.

19 See Stucke & Grunes, *supra* note 17, at 277; see also Pasquale, *supra* note 6, at 1009.

For firms, data (and access to it) bestows several significant and, in some cases, insurmountable competitive advantages over rivals.[20] Here we list two of the primary advantages. First, data has exceptional scaling effects. The more data that can be collected, the more inferences can be made about the subject matter providing the data.[21] The ability to make inferences based on the data collected dramatically enhances the ability of the data collector to offer a sellable product to customers, which, too, can be a significant driver in both acquiring and retaining users.[22]

For example, targeted advertising products are based on tech giants following users across the web — for the most part unbeknownst to them — to build near-comprehensive profiles advertisers use to reach them across various digital publications, whether they be the websites of *The New York Times*, and *The Wall Street Journal,* or mobile apps.[23] The inferences Google makes about users' behavior, based on their browsing history or navigational maps usage for example, are also incorporated into these profiles, something that other publishers cannot do and offer to advertisers.

Indeed, the scaling effects can be so significant that a market often moves toward consolidating to only one or several participants, increasing barriers to market entry as well.[24] In that case, potential firms would have to provide similar or superior service in order to have a successfully competing product — which is inexorably tied to data acquisition and the number of pre-existing users.[25]

Second, when data is the operating principle behind the development and marketing of products within the technology industry, access to it determines whether that product or service exists at all. For example, one of the reasons no meaningful competitor has been able to challenge Google's dominance in internet search is because, given bandwidth and website ownership limitations, only so many competing search engines can scan a website at a time to feed into search results.[26]

When combined, these factors incentivize technology giants to collect as much data as possible, integrate psychologically manipulative tactics and technical hurdles into products that make it difficult for consumers to switch providers, and degrade privacy protections so that more data can be extracted.[27] Firms that share their data can even act as gatekeepers and selectively choose who has access to their data or not, creating a sub-market that becomes heavily reliant on access to that data.[28] Such a situation creates an opportunity for market foreclosure, where a company is not able to compete effectively because its access to the data was closed off.[29] For example, when Vine, a precursor to the video-sharing platform TikTok, started to present itself as a competitor to Meta, Mark Zuckerberg personally shut off Vine's access to specific Facebook data channels.[30]

As a legal regime based on limiting access to data and defining the methods of how it is acquired, used, and sold, the market rules governing privacy, therefore, are a fundamental component of how technology markets are structured.

---

20 Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 Ariz. L. Rev. 339, 346-47 (2017).

21 Stucke, *supra* note 6, at 283.

22 *Id.* at 321; Eliana Garcés & Daniel Fanaras, *Antitrust, Privacy, and Digital Platforms' Use of Big Data: A Brief Overview*, 28 Competition: J. Anti., UCL & Privacy Sec. Cal. L. Assoc. 23, 24 (2018).

23 Hanley, *supra* note 16, at 311.

24 *Id.* at 282, 289-90; Pasquale, *supra* note 6, 1015-16; Salil K. Mehra, *Data Privacy and Antitrust in Comparative Perspective*, 53 Cornell Int'l L.J. 133, 140-41 (2020).

25 Hanley, *supra* note 16, at 289-91.

26 Daniel A. Hanley, *Let's Make Google Share Some Secrets*, Wash. Monthly (July 20, 2021), https://washingtonmonthly.com/2021/07/20/lets-make-google-share-some-secrets/; Allen P. Grunes & Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, 14 Antitrust Source, Apr. 2015, at 8.

27 Maurice E. Stucke & Allen P. Grimes, *Debunking the Myths over Big Data and Antitrust*, Competition Pol'y Int'l: Antitrust Chronicle, May 2015, at 1, 9; Stucke, *supra* note 6, at 285-86.

28 Stucke, *supra* note 6, at 304-05.

29 Hanley, *supra* note 16, at 322.

30 See Adi Robertson, *Mark Zuckerberg Personally Approved Cutting Off Vine's Friend-Finding Feature*, Verge (Dec. 5, 2018), https://www.theverge.com/2018/12/5/18127202/mark-zuckerberg-facebook-vine-friends-api-block-parliament-documents.

III. ANTITRUST IS AN ESSENTIAL LEGAL TOOL FOR SECURING CONSUMER PRIVACY RIGHTS AND STRUCTURING BUSINESS CONDUCT TO PROTECT PRIVACY

U.S. antitrust law originated in the late 19th century out of the need to restrain unfair practices engaged in by dominant corporations in order to preserve the vitality of the democratic governance of markets and promote nationwide economic opportunity.[31] Recognizing its general economy-wide application, Congress purposefully designed the antitrust laws to be exceptionally broad. Antitrust governs all aspects of firm rivalry and creates a legal floor of acceptable business conduct. Almost no method of competition is outside the purview of the antitrust laws.[32]

Antitrust law can target "every" unreasonable restraint of trade or monopolization tactic, as well as exclusive deals, tying, and mergers that "may be substantially to lessen competition, or tend to create a monopoly."[33] Giving additional strength to the antitrust laws is the Supreme Court's interpretation that the antitrust laws have "dynamic potential" not confined to particular practices and were to be aimed broadly at all of the "economic consequences" of business conduct.[34]

The restrictions on businesses imposed by the antitrust laws accomplish two primary goals. First, by limiting a plethora of business conduct, antitrust law ensures businesses are competing fairly, implicitly incentivizing firms to avoid unfair methods of competition and, instead, engage in socially beneficial conduct that maximizes benefits to the public. Such socially beneficial conduct can include increasing investments into research and development, increasing product quality, and increasing pay to workers. Second, antitrust prevents and remedies undue concentrations or exercises of corporate power that entrench and expand a firm's dominant control. Antitrust enforcement can thus promote competition, increase consumer choice, and enhance product quality.[35]

Endowed with exceptional flexibility regarding restricting unfair business practices, antitrust enforcement can complement privacy goals and facilitate notable privacy protections in at least three ways to ensure that corporations are protecting user data, ensuring the highest quality product to consumers, and engaging in fair competition regarding the gathering, use, or access to user data.[36]

First, antitrust enforcement, in general, can facilitate privacy protections by creating a market for privacy protections. Against the backdrop of decades of anemic antitrust enforcement and profound increases in market concentration since the 1970s,[37] a "race to the bottom" has occurred in the technology industry that has caused privacy-centric products to be unable to compete effectively against their data-dependent competitors and has allowed services to extract as much data as possible.[38]

For example, when it comes to search, social media, e-commerce, digital advertising, and a host of other markets, all are dominated by a few companies — and no meaningful competitor has emerged in decades.[39] Given the dependency on data for the technology industry, the prospect of obtaining a monopoly position by acquiring as much data as possible, and its essential role in supporting the creation of many products and services, it is clear that "natural" market forces geared toward data extraction are unable to provide consumers with robust privacy protections.

---

31 See 21 Cong. Reg. 3151, 1352 (1890) (statement of Sen. Hoar) (Section 2 of the Sherman Act regulates the "means which prevent other men from engaging in fair competition with him[.]")

32 Obviously, there are notable exemptions from the antitrust laws. See, e.g. 15 U.S.C. § 17 (exempting labor union activity from the antitrust laws).

33 15 U.S.C. §§ 1, 2, 13, 18.

34 *Bus. Elecs. Corp. v. Sharp Elecs. Corp.*, 485 U.S. 717, 731-32 (1988).

35 Sandeep Vaheesan, *The Profound Nonsense of Consumer Welfare Antitrust*, 64 Antitrust Bull. 1, 2-3 (2019).

36 *Nat'l Soc. of Pro. Engineers v. United States*, 435 U.S. 679, 695 (1978) ("all elements of a bargain - quality, services, safety and durability[.]").

37 See Michael Kades, *The State of U.S. Federal Antitrust Enforcemen*t, Equitable Growth (Sept. 2019); Gustavo Grullon et al., *Are US Industries Becoming More Concentrated?* 23 Rev. Fin. 697 (2018).

38 Grunes, *supra* note 14, at 1112; Hanley, *supra* note 16, at 303-05.

39 Hanley, *supra* note 16, at 346-49.

By being able to increase competition in an industry and prohibiting a myriad of business practices that cause adverse effects on consumers and market competition,[40] antitrust law fundamentally shapes and incentivizes how businesses compete and the methods of competition they use to succeed in the marketplace.[41] In other words, antitrust law, like privacy protection, is essential to structuring a market — in this case, creating the market conditions necessary to make privacy a feasible goal for firms to provide to consumers, and inhibit firms from invading a user's privacy and use data in unfair ways that entrench or expand a firm's dominance.[42]

Second, antitrust enforcement can ensure privacy protections by targeting three types of violative conduct — mergers, monopolization tactics, and deception. Technology companies have long used mergers as an essential method of competition to acquire data and entrench their market position. Between 1987 and 2019, Google, Meta, Microsoft, Apple, and Amazon acquired 760 companies.[43] Evidence shows that mergers have been critical to degrading privacy protections. For example, before being acquired by Meta, the communications service WhatsApp was a leader in offering consumers robust privacy protections.[44] Soon after its acquisition, Meta degraded privacy protections on WhatsApp, bundling customers' data into their main Meta social network profile.[45]

Since merger enforcement takes a broad review of transactions extending into increased prices, reduced output and quality, or adverse effects on innovation,[46] merger enforcement is particularly well positioned to promote privacy protections. Most importantly, merger enforcement directly prevents increasing market concentration and inhibits the loss of consumer choice.[47] Preventing market concentration has multiple positive effects: averting the loss of competitors, preventing the aggregation of data that can multiply the number of channels to collect it, and ensuring that proper market incentives exist so that competitors can implement privacy protections as a way to differentiate their product quality.[48]

Merger enforcement can also promote privacy protections by imposing strict settlement requirements. Antitrust enforcement agencies have broad authority to structure settlements in the public interest and can impose requirements on merging firms to maintain certain practices that protect user privacy or incur hefty fines or structural breakups.[49]

Antitrust enforcement can also facilitate privacy interests by targeting various methods of monopolization. As described above, privacy protections are a non-price indicator of product quality and can also be an indicator of product innovation. While using the degradation in privacy as the primary means to establish whether the violative conduct produces sufficient adverse effects to show harm to the "competitive process" would be difficult,[50] such a legal avenue is still available and indeed necessary to assert given that many of the products and services at issue are provided for free to users.[51]

Concerning enforcement against deception, while the evidence clearly shows that providing consumers the opportunity to agree to terms of service that detail a firm's privacy policies is woefully ineffective at securing their desire for inhibiting the gathering of their data and

40 See U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines § 1, at 2 (2010). (discussing how antitrust law can analyze price and non-price effects like decreasing quality, reduced service, and declining innovation).

41 H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial, and Administrative Law, 117th Cong., Investigation of Competition in Digital Markets: Majority Staff Rep. and Recommendations 12 (2022) (hereinafter "House Report").

42 David Millon, *The Sherman Act and the Balance of Power*, 61 S. Cal. L. Rev. 1219, 1264 (1988); Stucke, *supra* note 6, at 288-89.

43 Hanley, *supra* note 16, at 349.

44 FTC Facebook Complaint at 41.

45 *Id.* at 49.

46 John M. Newman, *Antitrust in Zero-Price Markets: Applications*, 94 Wash. U.L. Rev. 49, 58 (2016).

47 See generally Peter C. Carstensen & Robert H. Lande, *The Merger Incipiency Doctrine and the Importance of "Redundant" Competitors*, 2018 Wis. L. Rev. 781 (2018).

48 House Report, *supra* note 41, at 39 ("[In] digital markets…[t]he best evidence of platform market power therefore is not prices charged but rather the degree to which platforms have eroded consumer privacy[.]").

49 See, e.g. Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook; *United States v. Am. Tel. & Tel. Co.* (AT&T), 552 F. Supp. 131, 139 (D.D.C. 1982), *aff'd sub nom. Maryland v. United States*, 460 U.S. 1001 (1983) (Breaking up AT&T into seven telephone companies and a long-distance carrier); 15 U.S.C. § 16(e) (requiring settlements entered into by the United States to be in the public interest).

50 *NYNEX Corp. v. Discon, Inc.*, 525 U.S. 128, 135 (1998); Grunes & Stucke, *supra* note 26, at 8-9.

51 Hanley, *supra* note 16, at 279.

making consumers aware of how their data is collected and used,[52] antitrust enforcement can serve as a bulwark to ensure the minimal notice-based protections afforded to consumers are operating (at least to the extent they possibly can) for the benefit of the users.

The bare minimum requirement of proper notice to consumers is that it accurately and meaningfully conveys how their data is being collected and what it is being used for. Since data can provide such significant monopolization capabilities, a firm can easily justify pursuing deception and other nefarious practices on the grounds that short-run legal troubles — such as breach of contract or tarnishment of their brand — are worth the durable and dominant position that can be obtained in the future.[53] Considering the extensive harms caused by deception to consumers and market competition, including the "lack [of] any redeeming economic qualities or cognizable efficiency justifications," such conduct is well within the purview of the antitrust laws.[54]

Third, antitrust enforcement – both through full trials on the merits and through settlements – can pursue, and courts can grant, broad structural remedies that facilitate privacy protections. The federal courts possess remarkably broad remedial authority to address the adverse effects of the litigated antitrust violations to "cure the ill effects of the illegal conduct, and assure the public freedom from its continuance. Such action is not limited to the prohibition of the proven means by which the evil was accomplished, but may range broadly through practices connected with acts actually found to be illegal."[55] Court injunctions can and indeed must be designed to stop the violative conduct, inhibit it from occurring again from both the current and potential violators, and ensure the conditions of a market are conducive to real competition between firms.[56] Such structural remedies can break apart and inhibit the collection and aggregation of user data and create a market that can facilitate privacy interests.

IV. CONCLUSION

As long as technology companies rely on user data as the fundamental basis for their products and services, the rules governing privacy will always be a relevant and necessary discussion. A comprehensive federal law is long overdue in the United States, but federal antitrust enforcers have tools to ensure that in the meantime consumer privacy interests are protected.

52 Stucke, *supra* note 6, at 289.

53 Maurice E. Stucke, *How Do (and Should) Competition Authorities Treat a Dominant Firm's Deception?*, 63 SMU L. Rev. 1069, 1087, 1098, 1102 (2010); Note, *Deception as an Antitrust Violation*, 125 Harv. L. Rev. 1235, 1238 (2012) (hereinafter "Deception Note"); *United States v. Microsoft Corp.*, 253 F.3d 34, 76-77 (D.C. Cir. 2001); *McWane, Inc. v. FTC*, 783 F.3d 814, 838 (11th Cir. 2015).

54 Deception Note, *supra* note 53, at 1245-55.

55 *United States v. United States Gypsum Co.*, 340 U.S. 76, 88-89 (1950); see also *California v. Am. Stores Co.*, 495 U.S. 271, 294 (1990) ("[The Clayton Act's injunction provision] should be construed generously and flexibly pursuant to principles of equity").

56 *United States v. Grinnell Corp.*, 384 U.S. 563, 577 (1966) (stating that "adequate relief in a monopolization case should . . . break up or render impotent the monopoly power."); *Nat'l Soc. of Pro. Engineers*, 435 U.S. at 698 (An injunction is judged in part on whether "the relief represents a reasonable method of eliminating the consequences of the illegal conduct."); *United States v. E. I. du Pont de Nemours & Co.*, 366 U.S. 316, 326 (1961) (Relief must "restore competition."); *Ford Motor Co. v United States,* 405 U.S. 562, 575(1972) (The remedy should "cure the ill effects of the illegal conduct[.]") (internal citations omitted).

HOW CAN COMPETITION POLICY AND PRIVACY PROTECTION POLICY INTERACT?

BY GIULIANA GALBIATI & HENRI PIFFAUT[1]

1 Giuliana Galbiati is an adviser to the president of the Autorité de la concurrence. Henri Piffaut is a vice president at the Autorité de la concurrence. The views expressed in this article are those of the authors and do not represent those of the French Autorité de la concurrence.

I. WHY COMPETITION POLICY IS LIKELY TO INTERACT WITH OTHER PUBLIC POLICIES, AND WITH PRIVACY PROTECTION IN PARTICULAR

The perception of the interaction between competition policy and privacy protection has significantly evolved in recent years. While some initially argued that privacy was a distinct and complex issue and that competition enforcement should look the other way, market realities and digitization have since then forced regulators to reflect upon how the two policies can be interrelated and increase their coordination efforts. Regulations like GDPR try to give substance to privacy rights through definition of mandated levels of protection and consent. With the ensuing decrease in the asymmetry between platforms and users, privacy protection can become a relevant competition parameter. The question is then how to best inform competition policy of privacy issues. This paper examines possible answers.

Finding workable intersections between competition policy and other policies is not new. Just recently, there have been in-depth exchanges between EU competition authorities, including the Autorité de la concurrence (the "Autorité"), on how we can support the objectives of the European Green Deal in the framework of competition law. The European Commission's (the "Commission" or the "EC") revised HBER guidelines, which will include a specific chapter on sustainability agreements, as well as the revised guidelines on "State Aid for climate, environmental protection and energy 2022"[2] are concrete steps forward in this area. Even on the much-debated relationship between competition and industrial policies, there are several examples showing that the two can usefully complement each other. The recent hydrogen investment project known as IPCEI 2, approved by the Commission under state aid rules in July 2022, shows that it is possible to implement a modern industrial policy (here to strengthen Europe's position as a leading region for the hydrogen industrial transformation) while bringing competition on a newly created market. In fact, it could be argued that it is consubstantial to competition policy to interact with other policies that affect the competitive process.

In France, the legal framework has been designed to take into account the need for interaction between different policy objectives and regulators. The parliament, the government as well as sector regulators may or must (depending on circumstances) seek the opinion of the Autorité when legislative reforms or regulatory texts relating to competition are being prepared, or to explore ways of improving the competitive functioning of a sector or of specific geographical areas.

Conversely, in the antitrust area, the Autorité has a legal obligation (under article R.463-9 of the French commercial code) to consult sectoral regulators, by sending to them, when relevant, formal complaints or *ex-officio* decisions to open an investigation. Regulators may provide comments within two months. The Autorité has frequently used this mechanism in cases where privacy considerations were particularly relevant, as in the *Apple ATT* case (see below) with the CNIL, the French data protection regulator. As regards merger control, the legal obligation to consult sectoral regulators only applies with respect to the media industry (ARCOM)[3] and the banking and insurance industry ("ACPR")[4] in phase 2 proceedings. Of course, case teams always have the possibility to informally consult the data protection regulator in both phase 1 and phase 2 proceedings, as was recently done in the *TF1/M6* TV merger case.[5]

Beyond the enforcement of cases, we are witnessing a general movement towards the strengthening of cooperation between competition and privacy regulators. For instance, in the UK, the data protection authority, the ICO, and the CMA issued a joint statement in May 2021, presenting their common views on the relationship between competition and data protection in the digital economy. They emphasized the complementarity of the two regulatory frameworks, and affirmed their willingness to work together to find appropriate regulatory solutions.[6] This is notably the case in their joint review of *Google Chrome privacy sandbox* (see below). In France, where formal cooperation is already significant in both the advisory and enforcement frameworks, the Autorité and the CNIL have also engaged in other types of interaction, including presentations to the respective boards, cross-trainings of the investigation teams and joint workshops.

2 Communication from the Commission, Guidelines on State aid for climate, environmental protection and energy 2022, 2022/C 80/01, published in the OJEU on February 18, 2022.

3 Article 41-4, loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

4 Article L612-22, French Code monétaire et financier.

5 Autorité de la concurrence, press release, *TF1/M6: The Autorité de la concurrence takes note of the decision to withdraw its planned acquisition*, September 16, 2022.

6 "Competition and data protection in digital markets: a joint statement between the CMA and the ICO," 19 May 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf.

As President Coeuré recently pointed out before the board of the CNIL, while the objectives pursued by competition law and privacy regulation differ, the two regulatory frameworks nevertheless present a certain convergence, in that they are ultimately implemented for the benefit of consumers.[7]

On the one hand, competition policy aims to guarantee the conditions for free and undistorted competition between companies, by promoting innovation, diversity of supply and attractive prices. It should be stressed that the role of competition policy is somewhat special in that its policy objective is very broadly defined and potentially may intersect with any public policy that may have an impact on consumers or companies' behaviors. It is also specific in that the responsibility for enforcement and policy has been granted to an independent entity, at least in Europe and in France. Other public policies have in general a more focused objective and sometimes rely only on the judicial system for their enforcement, as opposed to a dedicated agency.

On the other hand, privacy policy aims at ensuring personal data protection, defining when, how and to what extent information about a person can be collected, processed, and communicated by and between undertakings. Privacy law, such as the GDPR, provides basic protection to individuals and data subjects, and affords rights to better control their personal data. Most jurisdictions operate a consent-based regime, which provides consumers with the ability to control how their data are collected and used by agreeing or withholding their consent.

However, companies design the choice architecture that leads to such consent, and this may influence the extent of the possible choice. In addition, in some jurisdictions, data protection legislation, as in the case of the GDPR, confers other rights, including the right to data portability. Again, the reality of that right will depend in part on companies' behavior and on privacy regulatory design. Both the relevant information on privacy and data portability can have significant effects on competition. Such legislation and implementing measures create a space where, theoretically, individuals can exercise a choice over the level of protection provided on their personal data and also allows comparison between undertakings on the level of protection offered. By doing so it opens privacy protection to become a genuine competition parameter.

The level of privacy protection would become a relevant competition parameter once meeting the legal requirements with regards to privacy protection (what can be called "mandated privacy protection"). Since these levels of protection have been mandated, all players on the market shall equally comply with the same requirements. However, if there are discretionary elements in how to implement the protection of basic privacy, there can be competition among different players on that basis. In addition, competition plays fully for the provision of privacy protection that goes beyond mandated levels. There is however the caveat of who would decide the mandated level has been achieved or the choice architecture is a real one. If the regulatory setting does not allow clear and quick conclusions on these, there would be a need for determination in a competition enforcement case.

Conversely, it could also be argued that lack of implementation of a privacy regulation could be seen as an infringement under both competition law (for instance where it constitutes an abuse of dominance) and privacy regulation. The most striking example of this scenario is the 2019 Facebook case before the Bundeskartellamt (discussed below). The Google related rights decisions by the Autorité[8] - even though they fall outside the scope of privacy regulation - are also a relevant example of how infringing or circumventing a regulation (in this case the European directive on related rights and the implementing French regulation) can possibly result in a violation of competition law.

Moreover, provisions such as data portability may lower (at least theoretically) switching costs for individuals if they want to change providers. "Theoretically » because for portable data to be useful, it should follow some standards in definition and format. It does not seem that we are yet there."[9] Conversely, the provision of privacy protection can become a way to raise barriers to entry. A company that controls a bottleneck in providing access to competitors to a market could structure the choice architecture for individuals to grant consent in such a way that individuals would be disinclined to grant consent. This is basically the claim of complainants asking for interim measures in 2020 in the *Apple ATT* case (the case has continued its life since then and this article does not take any stance on facts or law in that regard).

7 Speech of the president of the Autorité de la concurrence, Benoît Coeuré, before the CNIL, June 2, 2022, https://www.autoritedelaconcurrence.fr/sites/default/files/2022-06/20220608-CNIL-discours_0.pdf.

8 Décision n° 20-MC-01 du 9 avril 2020 relative à des demandes de mesures conservatoires présentées par le Syndicat des éditeurs de la presse magazine, l'Alliance de la presse d'information générale e.a. et l'Agence France-Presse ; décision n° 21-D-17 du 12 juillet 2021 relative au respect des injonctions prononcées à l'encontre de Google dans la décision n° 20-MC-01 du 9 avril 2020 ; décision n° 22-D-13 du 21 juin 2022 relative à des pratiques mises en œuvre par Google dans le secteur de la presse.

9 Case T-604/18, judgment of the General Court, 14 September 2022, §184: "In this regard, first, it should be observed that user loyalty to Android was not attributable, according to the Commission, solely to the quality of the OS. As the Commission indicated on the basis of the statements of OEMs cited in recitals 524 and 534 of the contested decision, the high degree of user loyalty to Android could also be accounted for by the difficulties users encountered in porting personal data or by the need to repurchase apps. In particular, as noted inter alia by one of those OEMs, users get used to the way their smart device works and do not want to relearn a new system (see recital 534(3) of the contested decision). User loyalty could not, however, be attributable to the quality of the OS alone, as the Commission stated in recital 488 of the contested decision, since many users were using Android versions that had not been updated."

Apple had announced in June 2020 its intention to implement a mechanism called ATT (App Tracking Transparency) by September 2020. This mechanism displays a pop-up window which requires the explicit consent of the iPhone user before any use of their "Identifier for Advertisers." This unique identifier allows online advertising companies to track users' activity on different websites or mobile apps, for the purposes of targeted advertising. The complaint filed before the Autorité asking for interim measures argued that the ATT prompt would constitute an abuse of a dominant position because it would be neither necessary nor proportionate to achieve Apple's objective of protecting users' privacy. The Autorité rejected the request for interim measures but decided to investigate the merits of the case.[10]

While it is therefore apparent that competition and privacy policies interact in many instances, the relationship between the level of privacy protection and the level of competition is not necessarily obvious. Indeed, competition policy seeks to address a market failure according to which firms may tend, collectively or unilaterally, to abuse market power and deprive consumers from the benefits of competition. In this context, offering a high level of privacy protection (mandated or not) may be a way to increase barriers to entry for competitors, as illustrated by the debate over Apple's introduction of ATT. Alternatively, a lower level of privacy protection may enable a firm to increase its returns over a dataset across markets, and may be tested once a company faces lower competitive constraints.

A consequence of this is that competition enforcement is not as efficient a tool to address privacy issues as privacy regulation. For example, the design of competition remedies usually looks at the root cause of market power that created the ability and incentive for the undertakings concerned to restrict competition. If an agreement or a unilateral action were found to restrict competition because they materially decreased privacy protection (while still meeting mandated obligations), a cease and desist order would be efficient to eliminate the ability to restrict competition only if accompanied by a monitoring akin to dedicated regulation; it would however be difficult to eliminate the incentive to behave in this harmful way, since it does not necessarily find its source in market power.

II. SCENARIOS WHERE COMPETITION POLICY AND PRIVACY POLICY ARE INTERRELATED/ INTERDEPENDENT

We identified three possible approaches in order to take into account privacy considerations in a competition law assessment: consider the two policies as autonomous and ignore; acknowledge that there is a coordination issue but defer its resolution to the privacy regulator and then adjudicate on the competition matter; or take an informed stance on the privacy issue that can serve as a basis for the competition assessment.

As for the first, the old stance claiming that, since each public policy has its own objectives, they should more or less ignore each other does not seem sustainable anymore. This is the approach that the European Commission followed in its 2008 review of the *Google/DoubleClick* merger in the online advertising industry, where one of the three non-horizontal theories of harm concerned the combination of Google and DoubleClick's data collection. The decision states that the Commission's review was limited to assessing whether the transaction would not impede effective competition, and was without prejudice to other obligations imposed onto the parties in the area of privacy and data protection.[11]

This was consistent with the Court ruling in the *Asnef Equifax* case, where the Court had to examine whether agreements concluded for the purpose of setting up credit information registers in Spain were potentially restrictive of competition and whether they could be exempted on the basis of Article 101(3). When examining the existence of a restriction of competition, the Court observed that it was not relevant to take into account privacy considerations in the context of the competition assessment: *"any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection," before adding however that it was "apparent from the documents before the Court that, under the rules applicable to the register, affected consumers may, in accordance with the Spanish legislation, check the information concerning them and, where necessary, have it corrected, or indeed deleted."*[12]

Similarly, in the 2014 F*acebook/WhatsApp* case, the Commission assessed the possible concerns associated with the combination of the two entities' datasets to determine whether it could constitute an obstacle to competition in the online advertising market. It pointed out however that it *"analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of*

10 Décision n° 21-D-07 du 17 mars 2021 relative à une demande de mesures conservatoires présentée par les associations Interactive Advertising Bureau France, Mobile Marketing Association France, Union Des Entreprises de Conseil et Achat Media, et Syndicat des Régies Internet dans le secteur de la publicité sur applications mobiles sur iOS.

11 Case M.4731 – *Google/DoubleClick*, March 11, 2008, paragraph 368.

12 Case C-238/05, judgment of the Court, November 23, 2006, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v. Asociación de Usuarios de Servicios Bancarios (Ausbanc),* paragraph 63.

Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."[13]

With the digitization of the economy, the use of personal data has become pervasive. The role of data and consequently consumers' preferences with regard to their privacy cannot anymore be separated as a rule from a competition assessment. Today most industries rely at least to some extent on data. It can be at the stage of the production process, at the commercial stage, for instance to improve marketing, or in the way products or services are sold. Digitization has also enabled the development of platform businesses.

A platform can be seen as an enabler for transactions between sides to take place. For the match to take place and then the transaction to be completed, a platform relies on data provided by both sides. From a competition standpoint, the accumulation of data can constitute an important source of market power. Very often such datasets may include personal data and therefore their use may raise privacy protection issues. This is even more the case when the platform includes a "data side," i.e. uses or grants access to personal data to provide targeted advertisement. In addition, as discussed earlier, the adoption of privacy protection legislation based on information of consumers and seeking their consent has led to consumers being better able to compare and express preferences in relation to levels of privacy protection.

The second approach is akin to the solution adopted in IP matters: a competition authority may find a patent to be obviously invalid but may not take a stance on validity or infringement beyond finding that there is uncertainty on the outcome of disputes. Since most conflicts in IP are adjudicated through court proceedings, such an approach may make sense. In privacy matters, where a dedicated regulator has been attributed some monitoring powers, this approach would present the drawback that available expert opinion would not be sought in the course of competition proceedings.

The third approach would go further than the second in allowing to make a finding based on exchanges with the privacy regulator. That is the approach that the Bundeskartellamt followed in its *Facebook* case, where it considered that imposing on users the aggregation of their data in violation of the provisions of the GDPR constituted an exploitative abuse of Facebook's dominant position. The legality of this approach is one of the questions put to the European Court of Justice in the request for a preliminary ruling from the Higher Regional Court of Düsseldorf. Advocate General Rantos rephrased that question in the following way: "[may] *a competition authority (…) examine, as an incidental question, the compliance of the practices under investigation with the GDPR rules, while taking account of any decision or investigation of the competent supervisory authority on the basis of the GDPR, informing and, where appropriate, consulting the national supervisory authority"*?[14] His proposed answer is "yes," noting though that the competition authority could "possibly" wait for the outcome of the privacy regulator investigation and its findings could not bind the regulatory authority.

In the following we first examine to what extent privacy could be taken into account when it is not considered as a competition parameter and then look at the situation where it would be a competition parameter.

III. WHERE PRIVACY PROTECTION IS NOT A RELEVANT COMPETITION PARAMETER FOR THE ASSESSMENT OF A PRACTICE, BUT…

The conduct in question (negatively) affects both competition (in terms of prices, quality, innovation, etc.) and privacy. Even where privacy protection would not be a competition parameter, a given conduct or merger could still affect in parallel both competition and privacy. In this scenario, the competition agency should focus its efforts on solving the competition issue; however this might also have an impact on privacy considerations, and it would not seem appropriate that the two policies ignore each other. The definition of appropriate measures in both areas should somehow be coordinated.

For instance, in its *Google/Fitbit* merger decision[15] the Commission looked at the impact of the aggregation of Fitbit's health and fitness user data with Google's existing datasets. It found no evidence that privacy was a parameter of competition for wearable devices and accordingly, did not include privacy in its substantive assessment of the transaction. In addition, it presumed that Google and Fitbit would lawfully combine their databases under privacy law. Should such presumption prove to be incorrect, the *"effects of the transaction […] would be the same, but the parties remain accountable for any breach of GDPR or the e-Privacy Directive."* Obviously, this assessment relies on the assumption that privacy would continue in the future not to be a parameter of competition in that field.

13 Case M.7217 – *Facebook/WhatsApp*, October 3, 2014, paragraph 164.

14 C-252/21, Opinion of Advocate General Rantos, September 20, 2022, *Meta Platforms and Others*, paragraph 33.

15 Case M.9660 – *Google/Fitbit,* December 17, 2020.

The conduct in question is pro-competitive but negatively affects privacy protection. When a conduct or merger is pro-competitive, competition law does not apply, and it would be for the privacy regulator to address any issue under privacy law in order to evaluate whether privacy regulation has been violated. It could be argued that the privacy regulator should however make sure that any negotiated settlement over privacy protection would not lead to restrictive effects on competition and limit the *effet utile* of competition law.

The conduct in question restricts competition but is compliant with privacy regulation and/or positively affects privacy protection. Alternatively, when a conduct or merger restricts competition but at the same time impacts positively privacy protection, there is no balancing exercise to undertake among several competition parameters to assess the effect on competition, since privacy protection is not a competition parameter. A balancing exercise could however take place under Article 101(3) or as a second step in the analysis under Article 102. The first condition under Article 101(3) states that the agreement or concerted practice in question should contribute to improving the production or distribution of goods or to promoting technical or economic progress.

That would seem to include a public policy objective such as protecting privacy. This is dependent on checking whether the envisaged measures do really enhance privacy protection which may require expert opinion. Privacy protection would likely be accepted to fulfill the second condition of Article 101(3), i.e. that the agreement should allow consumers a fair share of the resulting benefit. The third and fourth conditions, related to the indispensable nature of the restriction and the fact that the agreement shall not eliminate competition in respect of a substantial part of the products in question, would amount to a proportionality test whereas the undertakings concerned would have to show that there are no other ways to achieve the same objective that would less restrict competition. A similar exercise could take place under Article 102. Usually solving such an issue would cause a variation in the level of privacy protection. This is discussed in the next scenario.

The conduct in question restricts competition and the measures envisaged to remedy the competition issue may involve privacy protection considerations. The last possible scenario that we identified would be when a conduct or merger would restrict competition (with no plausible justification under privacy protection) and solving the competition issue could lead to a variation in the level of privacy protection. Clearly the competition agency could not impose measures that would violate privacy protection rules. However, when the variation in privacy protection would be negative while not infringing privacy rules, what should the competition agency do?

First of all, it should be underlined that compliance or not with privacy rules may not be obvious to assess. In that case, it would seem desirable, save for confidential information, that competition agency would consult with the competent privacy protection agency to check that aspect. As mentioned above, such consultation rules exist under French law, however, in the antitrust area, it is only required by law when the formal complaint or the decision to open an *ex-officio* investigation relate to sectors falling within the areas of expertise of the CNIL. In addition to the fact that privacy regulation can hardly be regarded as a sector, it may not be easy to know, at that early stage of the proceeding, that the measures that will later on be envisaged to remedy the competition issue will have an impact on privacy protection rules. In this respect, such scenario does not necessarily entail a mandatory consultation of the CNIL, but the investigation team might still wish, at the remedy stage, to contact the data protection agency on an informal basis.

Assuming now that the variation in privacy protection caused by the resolution of the competition issue would not lead to compliance issues, the question remains to what extent the competition agency should, ceteris paribus, favor a solution that would harm the least privacy protection. After all, the European legislator has granted a special status to privacy protection.

In this context, privacy rules may act as an external constraint on the design of merger remedies. Access to a dataset could both lower barriers to entry and risk running contrary to privacy rules. For instance in *Google/Fitbit*, the EC conditioned clearing the transaction on Google's commitment to provide users with an effective choice to: (i) grant or deny the use of certain Fitbit data by Google services; and (ii) allow third parties' access to the data types made available in the Fitbit Web API, subject to certain privacy and security requirements. In France, the Autorité informally consulted the CNIL in its *Enerest/Electricité de Strasbourg* case[16], in order to ensure the compliance with privacy regulation of a data access commitment, whereby the parties (two historical suppliers of gas and electricity) committed to send every competitor that would request it the necessary customer information to design their own offers.

Similarly, in some conduct cases, the Autorité was constrained in remedying a restriction of competition because of privacy protection considerations. Two relevant French cases include the *GDF-Suez* case[17] and the recent EDF case,[18] both in the energy sector. In the first one, the

16 Décision n° 12-DCC-20 du 7 février 2012 relative à la prise de contrôle exclusif d'Enerest par Electricité de Strasbourg, see §89.

17 Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité (interim measures decision); décision n° 17-D-06 du 21 mars 2017 relative à des pratiques mises en œuvre dans le secteur de la fourniture de gaz naturel, d'électricité et de services énergétiques (decision on the merits).

18 Décision n° 22-D-06 du 22 février 2022 relative à des pratiques mises en œuvre par la société EDF dans le secteur de l'électricité.

CNIL was formally consulted by the Autorité under article R.463-9 of the French commercial code in light of the data-related concerns expressed by a competitor (Direct Energie) in its formal complaint and with respect to the interim measures that the Autorité was considering.

These measures consisted of the incumbent granting its competitors an access to some of the data it had collected as a provider of regulated offers, in order to ensure effective competition on a separate market that had recently been opened to competition. The CNIL provided relevant information with respect to the data that could be shared as well as the process that had to be put in place to collect customers' approval to such data sharing. In the 2022 EDF case, EDF decided to settle an abuse of dominance case and offered a series of commitments, including the sharing of its customer file on the relevant market with alternative electricity suppliers who requested it. The CNIL was informally consulted on the commitments' proposal, and it is apparent from their final drafting that privacy protection considerations were taken into account by EDF.[19]

It is worth stressing that the design and monitoring of remedies that would involve requiring consent for privacy protection reasons would need to pay particular attention to the choice architecture followed when seeking consent. If not properly designed these remedies could lead to additional barriers to entry.

IV. WHERE PRIVACY PROTECTION IS A COMPETITION PARAMETER

It is now widely accepted that privacy protection (beyond its mandated level) has become a possible competition parameter. One of the early manifestations of this was Facebook's growth at the expense of MySpace. At the time, Facebook advertised its services as better able to protect users' privacy than that of MySpace, the incumbent.

In its recent judgement on the Commission's decision in the *Google Android* case, the General Court acknowledged that *"variables other than technical quality, such as the protection of privacy (…) also play a role"* (para 578). It has also been argued that infringement of privacy regulation could amount to a competition law infringement (see discussion above with regard to the 2019 Facebook case before the Bundeskartellamt).

Consumers could therefore consider privacy protection as a relevant competition parameter, in particular where players can exercise discretion in deciding how to implement privacy regulation or where they decide to go beyond what is legally required. In a way equivalent to the assessment of impact on quality, the effect on competition of a certain conduct or merger should then consider the impact on privacy protection.

Accepting that privacy protection would amount to a competition parameter leads to some balancing exercise of the effects of an agreement, a unilateral action or a merger on that parameter and other parameters such as quality, quantity, price, etc. It is the outcome of this balancing that would lead to the conclusion that there is a restriction of competition. Whereas in the case of two independent policies, the balancing would take place in the form of a proportionality test (if there was first a restriction of competition), here it would be a more in-depth analysis at the first stage of the competition law assessment, i.e. under Art 101(1) or Art 102 prior to the examination of efficiency or objective justifications. However, there would still be an assessment at the second stage of the competitive assessment, as discussed above. Several scenarios could be envisaged in this context.

The conduct in question would harm certain parameters of competition while leading to an increase in privacy protection (beyond what is mandated by law). This scenario would need to pass a first stage analysis before the proportionality assessment described above: the competition agency would have to determine whether the overall effect would be restrictive or not. This would be an evaluation similar to that of ancillary restraints.

As stated in *MasterCard*, a restriction is ancillary when an operation that is not anticompetitive in nature, would be impossible to carry out in the absence of the restriction in question. It would not be enough if the operation were more difficult to implement or less profitable without the restriction.[20]

The conduct in question would harm several competition parameters*, including privacy.* In this scenario, where a given practice would therefore infringe competition law at the first stage of the analysis, the competition authority and the data regulator would have to coordinate very closely if only to determine the level of harm on privacy and whether mandated privacy is involved. In the antitrust area, it is conceivable that the competition agency would decide to let the privacy regulator deal first with the issue. However, that would require two prerequisites: that the issue is mostly one of privacy protection and that the regulator would be competent, i.e. that the behavior would likely infringe privacy law. Such preliminary finding would mean that the two agencies would early on discuss the issue. In practice it seems unavoidable that the compe-

19 See for instance pages 3 to 7 of EDF's commitments and Annexes 1 and 2 attached to the decision.

20 C-382/12 P, judgment of September 11, 2014, *MasterCard and Others v. Commission*, paragraph 91.

tition agency would at some point have to take position, also in light of the fact that other competition parameters would be affected alongside privacy.

In the case of merger control, a competition agency would have no discretion to let a regulator deal with privacy issues when these are a competition parameter. In *Facebook/WhatsApp*,[21] the Commission found that privacy was an important parameter of competition in relation to consumer communication services. In *Microsoft/LinkedIn*, the Commission found that privacy was a *"significant factor of quality"* and therefore an important parameter of competition and "*driver of consumer choice."* If the market for PSN services reached a "tipping point" in favor of LinkedIn after its combination with Microsoft, the Commission noted that this would restrict consumer choice in relation to privacy protection, an *"important parameter of competition"* according to its investigation, when choosing a PSN.[22] In that case the Commission posited that one effect of the merger would be a decrease in competition constraints from other players with better privacy protection. There was no examination of the relationship between market structure and incentive to protect privacy.

When privacy is a competition parameter, but the issue is mostly one distinct from privacy protection or when the effect on privacy is outside the scope of mandatory actions. In these scenarios the competition agency would need to make an assessment that would also cover privacy protection. Here again, a mechanism that would seek views from the privacy regulator over the effect of the behavior on mandated or not mandated protection and possible remedies over privacy protection would seem advisable. In addition, the developments above on how to solve the competition issue while minimizing negative effects on privacy protection remain relevant.

The UK CMA's review of Google's privacy sandbox, in coordination with the ICO, is a relevant example for cooperation between the two regulators.

Google, with its proposed "privacy sandbox," intended to change its web browser in order to address privacy concerns by replacing cross-site tracking of users (notably through cookies) with a set of alternative tools. The CMA was concerned that Google's privacy sandbox would lead to unequal access for third parties to the functionality associated with user tracking, Google "self-preferencing" its own ad tech providers and ad inventory, and the imposition of unfair terms on Chrome's web users. In addition, the ICO had its own concerns over the impact on data protection law and privacy outcomes for individuals.

The CMA explained that in assessing concerns and negotiating and designing remedies it had been "working closely" with the ICO. In addition, since the remedies were dynamic in nature, it would continue to consult the ICO to ensure that both privacy and competition concerns were addressed as the proposals were developed in more detail.

V. CONCLUSION

It is now clear that competition and privacy policies are interrelated. Against this background, there is a need for coordination to maximize outcomes of both policies. However, these policies operate within two distinct regulatory settings (on material competences and geographies) and that makes such coordination complicated: there is a risk that perceived regulatory failure on the privacy side be filled in by competition law enforcement.

It is also important to bear in mind that in Europe other legislative tools will be added to the existing regulatory framework in the coming months, which may increase the degree of complexity in dealing with this issue. The obligations imposed by the Digital Markets Act, see for instance article 5(2) of the regulation, will also play a key role in regulating the illegal practices of digital platforms with respect to the collection, combination, and use of personal data. The impact of the proposed Data Act, which aims to increase the fair use and sharing of data across all economic sectors, will also need to be taken into account.

Finally, one should not ignore the impact of evolving technology which may upend interaction between privacy and competition notably when access to datasets and portability are concerned.

21 Case M.7217 - *Facebook/WhatsApp*, October 3, 2014, paragraphs 87, 102 and footnote 79.

22 Case M.8124 - *Microsoft/LinkedIn*, December 6, 2016, paragraphs 349-351.

TOWARDS DATA PORTABILITY AND INTEROPERABILITY UNDER BRAZILIAN COMPETITION LAW: CRAFTING APPROPRIATE LEGAL STANDARDS FOR ABUSE OF DOMINANCE

BY VICTOR OLIVEIRA FERNANDES[1]

1 Commissioner of the Administrative Council for Economic Defense ("CADE") in Brazil and professor of Competition Law at the Brazilian Institute for Teaching, Development and Research ("IDP"). The author holds a Ph.D. Degree in Commercial Law from the University of São Paulo ("USP"). The author's opinions should does not represent the official positions of the institutions mentioned.

I. INTRODUCTION

The interaction between data protection and antitrust laws has become a vital topic for competition law scholars in recent years, as several agencies' reports have raised major concerns about reduced levels of data protection derived from market concentration.[2] Although antitrust and data protection regimes pursues different goals, which might even clash at their margins,[3] in some circumstances, both branches of law require convergence.[4]

A crucial area of complementarity between both regimes is ensuring greater mobility of data through data portability, interoperability, and open data standards in digital markets.[5] The creation of barriers to interoperability or data portability might at the same time constitute a violation of data protection legislations and an abuse of dominance under antitrust law.[6] Moreover, mandating interoperability is generally perceived as an effective antitrust remedy or regulatory measure to enhance competition in digital markets.[7]

But the perspective of complementarity around this topic still faces considerable challenges for antitrust authorities. Although the competitive implications of interoperability restrictions have been extensively explored, there is still very little guidance as to which legal standards should be adopted under the antitrust laws. This paper discusses how antitrust agencies would scrutinize impediments to interoperability or data portability as an abuse of dominance infringement. It delves into this topic against the backdrop of Brazilian competition and data protection law, given some insightful cases were brought under this jurisdiction in recent years.

In Brazil, the approximation of the two areas has been intensifying since the General Data Protection Law (Law no. 13,709) was issued in 2018. This law came into force in 2020 and is currently enforced by the National Data Protection Authority ("ANPD") which has the full responsibility for applying administrative sanctions for non-compliance with the legislation.

After the adoption of the Brazilian general data protection law ("LGPD"), the Brazilian Competition Authority took relevant steps towards enhancing cooperation with the data protection watchdog. In May 2021, for example, CADE, ANPD, the Federal Prosecutor's Office, and the National Consumer Secretariat issued a joint recommendation about how new privacy policy announced by WhatsApp for the instant messenger service posed risks for data protection rights and raise potential anticompetitive effects[8].

Also, after the LGPD was enacted, CADE ruled some relevant abuse of dominance cases involving the imposition of contractual or technical restrictions on data interoperability. Considering the Brazilian experience, this paper argues that the applicable legal standards for assessing this form of unilateral conduct should be eminently contingent upon the feasibility of the enforceable antitrust remedies.

The reason for this context-based approach lies in the ambiguous effects of interoperability measures on competition in digital markets. In circumstances where imposing interoperability proves futile to increase competition or even increase privacy and security risks, antitrust authorities should be cautious. In such cases, the applicable legal standards should require strong evidence of competitive harm.

---

2 For a comprehensive review of reports on competition policy in the digital economy, see Filippo Lancieri & Patricia Morita Sakowski, *Competition in Digital Markets : A Review of Expert Reports*, 26 Stanford Journal of Law, Business & Finance 65–170, 97–98 (2021) (showing that "multiple reports argue that lower privacy protections and increases in data collection are important forms of non-price competition that must be considered by antitrust regulators."

3 Erika M Douglas, *The New Antitrust/Data Privacy Law Interface*, 2280 The Yale Law Journal Forum 647–684, 658 (2021)

4 Francisco Costa-Cabral & Orla Lynskey, *Family ties: The intersection Between Data Protection and Competition in EU law*, 54 Common Market Law Review 11–50, 21–22 (2017) and Maria Wasastjerna, Competition, Data and Privacy in the Digital Economy: Towards a Privacy Dimension in Competition Policy? 139 (Kluwer Law International) (2020).

5 Maurice E. Stucke, Breaking Away: How to Regain Control Over Our Data, Privacy and Autonomy 157–165 (Oxford University Press) (2022) (discussing data portability, data openness, open standards and increased inter-operability as complementary policies to promote the flow of personal data in digital markets).

6 Organization for Economic Co-operation and Development - OECD, Data Portability, Interoperability and Digital Platform Competition 28 (OECD Publishing) (2021).

7 Stigler Committee on Digital Platforms, Stigler Committee on Digital Platforms Final Report 117 (Stigler Center for the Study of the Economy and the State) (2019); Competition and Markets Authority - CMA, *supra* note 2, at 24que é o anuncio que tem relação com o conteúdo que o usuário está visualizando naquele momento, e o anuncio "personalizado", que é o anuncio feito a partir de informações pessoais do usuário, seja a partir de informações que ele fornece voluntáriamente à plataforma, seja através do rastreamento da sua atividade pela web ao longo do tempo. \n\n(.... See also Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, H.R. 3849, 117th Cong. (2021)

8 Administrative Council for Economic Defense ("CADE"). *Cade, MPF, ANPD e Senacon recomendam que WhatsApp adie entrada em vigor da nova política de privacidade*. Available at https://www.gov.br/anpd/pt-br/assuntos/noticias/cade-mpf-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade.

On the other hand, where there are indications that interoperability and open data standards are not only beneficial for competition but also reasonably manageable, the antitrust authority should move the pendulum toward finding an abuse of dominance. In seeking to make this distinction, antitrust authorities are confronted with choices that can reshape the level of competition for digital product design.

In part II, we will briefly explain how Brazilian antitrust law leaves room for new theories of the harm of abuse of dominance in digital markets and how data portability and interoperability restrictions fit into these theories. In part III, we will discuss the dilemmas involved in imposing interoperability measures as antitrust remedies in digital markets.

II. DATA-RELATED ABUSE OF DOMINANCE THEORIES OF HARM UNDER BRAZILIAN COMPETITION LAW

Under Brazilian competition law, the prohibition of abuse of dominance is defined in art. 36 of the Competition Law in a generic way, as a prohibition of strategies by companies that may in any way threaten free competition, dominate relevant markets, or arbitrarily increase profits.

The notion of abuse of dominance is not restricted to economic relations based on monetary prices. Therefore, CADE has rendered important decisions in the control of unilateral conduct that reject the thesis that zero-price business models would have any kind of immunity.[9] Thus, digital platforms can be scrutinized as "antitrust markets" under the lens of Law 12,529 of 2011, as these platforms make economic exchanges based on data and attention costs.[10]

As in many digital markets the offering of products and services by advertising-based platforms does not involve monetary charges, one can assess the nature of economic exchanges between users and platforms by to simply replacing the unit "price" used in economic models of consumer surplus with other quantitative metrics that represents the respective costs related to the exchange of data between users and digital platforms.

Paragraph 2 of art. 36 of Law 12.529,2011 defines market power as the ability to “unilaterally or coordinately alter market conditions.” Under this broad perspective, digital platforms could exercise market power in very particular ways. Instead of setting monopoly prices, they can extract quantitatively more data, or limit costumer’s ability to share their data with other rivals.[11] In both cases, the platform’s ability to unilaterally impose significant and non-transitory increases on data-related costs signals the exercise of market power.[12]

New theories of harm for unilateral conduct can be drawn from addressing digital dominance under Brazilian competition law. Under an exploitative abuse of dominance perspective, major platforms can harm costumers by requiring quantitatively more data in exchange for digital services or imposing unfair terms of use and conditions.[13] As exploitative abuses have remained quite debatable under Brazilian competition law,[14] one arguably better approach is framing the abuse of dominant position of digital platforms through an exclusionary lens.

A dominant firm might be able to foreclose competition or raise rival's costs through preventing its users from achieving data portability or imposing limitations on data interoperability across platforms.[15] The alleged non-rivalry and non-exclusivity of the data do not crowd out the

9 For a review of CADE’s case law, see Victor Oliveira Fernandes, Direito da Concorrência das Plataformas Digitais: entre abuso de poder econômico e inovação 170–171 (Revista dos Tribunais) (2022).

10 John M Newman, *Antitrust in Zero-Price Markets: Applications*, 94 Washington University Law Review , 72–73 (2016).

11 Samson Y. Esayas, *Competition in (data) privacy: ’zero’-price markets, market power, and the role of competition law*, 8 International Data Privacy Law 181–199, 181 (2018) ("*market power may be exerted by reducing the level of data privacy*").

12 Jason Furman et al., Unlocking Digital Competition: Report of the Digital Competition Expert Panel 42 (2019)

13 Viktoria H.S.E. Robertson, Excessive Data Collection: *Privacy Considerations and Abuse of Dominance In The Era of Big Data, in Common Market Law Review*, 1, 57 , 2020, pp. 161–190.

14 Eduardo Pontual Ribeiro & César Mattos, *The Brazilian Experience with Excessive Pricing Cases: Hello, Goodbye*, Excessive Pricing and Competition Law Enforcement 173–188 (2018) (arguing that the non-autonomous nature of exploitative abuses infringements or its legal inefficacy led its removal as an abuse of dominance violation under the Law no. 12,529/2011).

15 Organization for Economic Co-operation and Development - OECD, supra note 5, at 25–27 and Stigler Committee on Digital Platforms, *supra* note 6, at 43.

merits of these theories of harm. Even if it is possible for the rival to achieve a minimum viable scale to operate its platform, impediments to data portability or interoperability can keep the monopoly power of dominant platforms unchallenged in a context of weak competition.[16]

Impediments on data portability or interoperability can take the form of contractual, behavior or even technological barriers.[17] These conducts can be framed under the examples contained in the non-exhaustive list of art. 36, § 3, items III and IV, of Law No. 12.529, 2011. Adopting terms that outright prohibit data transfer between platforms is a rare practice in most digital markets. However, dominant players may adopt some indirect practices aimed at restricting multihoming or switching between platforms. Some examples may include the implementation of cognitive barriers to data transfer from one platform to another, the bundling of complementary services around the dominant platform's ecosystem, or the provisions of benefits to users who adopt "single-homing" behaviors.

III. ESTABLISHING APPROPRIATE LEGAL STANDARDS FOR RESTRICTIONS TO DATA PORTABILITY AND INTEROPERABILITY

Dominant digital platforms may violate both data protection and antitrust laws by imposing restrictions to data portability and interoperability. In Brazil, the LGPD sets forth the right to data portability upon express request of the user, commercial and industrial secrets observed, and in accordance with the regulations to be issued by the national data authority (article 18).

The legislation also assigns to the ANPD the legal power to define interoperability standards for the purposes of portability, free access to data and security (article 40). In some specific regulated sectors in Brazil, such as financial services and health care, there are additional rules on data portability which are sometimes aimed at promoting competition.

However, it is not straightforward to establish the conditions under which an impediment to data portability or interoperability constitutes an infringement. So far, there is a relevant scholarship suggesting that such conducts may fall under some mature categories of abuse of dominance. Contingent on how dominant platforms hinder competitors from gaining access to user data, their conduct can be framed as tying or bundling practices,[18] exclusive dealing[19] or refuse to deal.[20] When such parallels are drawn, antitrust agencies tend to focus on how the criteria established in case law for the assigned category of abuse should be translated to assess the practice adopted by the dominant platform. The categorical thinking though may thus handicap a more comprehensive competitive analysis.

We argue that impediments to data portability or interoperability must be primarily evaluated against the background of the relevance of interoperable data for competition in the markets affected by the unilateral conduct. Antitrust agencies should be aware that competition is ambiguously affected by data portability or interoperability measures.

Greater interoperability can enhance competition both in the same relevant market in which the dominant platform operates and in complementary markets.[21] Moreover, it can level the playing field in competition for the development of more privacy-friendly technologies.[22] However, there are some instances which may render the portability or interoperability of data superfluous or even detrimental for competition.[23]

16 Steven C. Salop, *The Raising Rivalss Cost Foreclosure Paradigm, Conditional Pricing Practices and the Flawed Incremental Price-Cost Test*, 81 Antitrust Law Journal 371–421, 392 (2017)it may depend on the structure of the plaintiff's allegations. Some types of conduct, notably conditional pricing practices (CPPs ("A firm can achieve, enhance, or maintain monopoly power by raising the costs or restricting the output of rivals that remain viable, whether or not the rivals are able to reach the [Minimum Efficient Scale] MES level of output").

17 Daniel L Rubinfeld & Michal S Gal, *Acess Barriers to Big Data*, 59 Arizona Law Review 339–381, 366 (2017).

18 Organization for Economic Co-operation and Development - OECD, Abuse of Dominance in Digital Markets 42 (OECD Publishing) (2020).

19 Michael L. Katz, *Exclusionary Conduct in Multi-Sided Markets*, OCDE Rethinking Antitrust Tools for Multi-Sided Platforms 101–130, 114–115 (2018).

20 Wolfgang Kerber & Heike Schweitzer, *Interoperability in the Digital Economy*, 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 38–58, 51–52 (2017).

21 Jan Krämer, *Personal data portability in the platform economy: economic implications and policy recommendations*, 17 Journal of Competition Law & Economics 263–308 (2022) (assessing data portability as a solution for lowering switching costs in networks markets).

22 Stucke, *supra* note 5, at 162–163.

23 Chris Riley, *Unpacking Interoperability in Competition, in Journal of Cyber Policy*, 1, 5, 2020, pp. 94–106 (discussing six different ways in which interoperability implies opportunities to promote or to impede competition); Organization for Economic Co-operation and Development - OECD, *Data Portability, Interoperability and Digital Platform Competition*, 2021, p. 22-24.

In practice, granting free flows of access to costumer's data is not a silver-bullet for lowing barriers to entry, as many other factors may drive the choice of costumers of switching platforms.

Crafting data-sharing antitrust remedies requires then several factors to be weighed and balanced. The most relevant are the competitive importance of data, the innovation incentives, and the impacts of data-sharing measures on users' rights.[24] Because of that, antitrust authorities should focus on abuse cases where data-sharing remedies can enhance competition in both effective and sustainable ways.

We propose a general framework for analyzing unilateral conducts conceived to that goal. First, platform dominance needs to be founded within the market structure. A general classification discerns horizontal interoperability from vertical interoperability. Horizontal occurs between competing networks, services, and platforms, as vertical has to do with complementary products and services.

This very classification can help assess dominance. The investigated platform must at least have a dominant position in either the "origin" market or the "target" market of the conduct. The dominance threshold eventually distinguishes antitrust and data protection interventions, as the data protection authorities' enforcement is not confined to imposing regulatory measures on dominant firms.

Second, one must scrutinize if the dominant platform is capable of imposing restrictions on data portability or interoperability and if it has the economic incentives to do it. Even a dominant player may not be capable of preventing rivals from accessing relevant data for competition. That could be the case when regulatory open data standards are already in place, and rivals are not inherently dependent on the dominant platform.[25] Particularly puzzling then are situations where open data standards exist but are not being more effectively enforced. Competition authorities' intervention may be even more crucial in these instances, and no antitrust immunity should be granted.

From the incentive's standpoint, one should inquire whether such data being prevented from sharing is particularly relevant to competition. Refusing interoperability will be especially rewarding for the dominant platform when data access could help rivals to overcome network externalities or when the dominant platform aims to leverage market power to an adjacent market.[26] However, in some cases, the competitive advantage does not stem uniquely from the data directly provided by users but rather from the across-users set of data gathered within the platform.[27] In social networking markets, for example, there are significant doubts about whether the data potentially involved in interoperability measures would be relevant for competition.[28]

Third and finally, the economic justifications for the conduct must be carefully examined. Rationales should be assessed under two contextually based arguments, notably the incentives for innovation and risk and for privacy and safety. As regards innovation, in more mature markets where competition is primarily for low-differentiated services, restrictions on interoperability are hardly justifiable. But where competition for innovative features is strong, antitrust remedies can homogenize services and tip the market towards a dominant technological standard.[29] As for privacy issues, one should consider whether the ownership of the data subjected to mandatory imposition of interoperability is clear and definable.[30]

On top of that framework, the most critical aspect of the abuse of dominance review in these cases seems to regard the feasibility of applying interoperability antitrust remedies, both in design and administration. Some commentators have extensively discussed these challenges, attempting to pinpoint the scenarios where identifying and imposing these remedies would be best addressed via competition authorities or national regulators.[31]

---

24 Competition and Markets Authority - CMA, *supra* note 7, at 370

25 Stucke, *supra* note 5, at 163–165 (assessing the relevance of data openness for enhancing competition).

26 Kerber & Schweitzer, *supra* note 20, at 51–52.

27 Organization for Economic Co-operation and Development - OECD at 22 and Amelia Fletcher, *Digital Competition Policy: Are Ecosystems Different?,* OECD Hearing on Competition Economics of Digital Ecosystems , 4 (2020).

28 Gabriel Nicholas & Michael Weinberg, *Data Portability and Platform Competition: is user data exported from Facebook actually useful to competitors?*, NYU School of Law Engelberg Center on Innovation Law and Policy (2019).

29 Competition and Markets Authority - CMA, *supra* note 7, at 370

30 Nicholas & Weinberg, *supra* note 28, at 18.

31 Filippo Lancieri & Caio Mario da Silva Pereira Neto, *Designing remedies for digital markets : the interplay between antitrust and regulation*, 1 Journal of Competition Law and Economics 1–57 (2021).

Some practical examples from the Brazilian jurisdiction helps to understand these challenges. The first paradigmatic case worth mentioning is the antitrust probe launched in 2013 against Google for the so-called "AdWords Abuses."[32] Google was accused of imposing technical and contractual restrictions on their AdWords API licensing. The investigated constraints were alleged to impede software developers from offering advertisers campaign management solutions. Campaign management software would be prevented from interoperating the data provided to AdWords platforms with rivals (such as AdBing).

When the case was tried in 2019, CADE's Tribunal scrutinized the existing provisions in Google's AdWords API licensing agreement, which had previously been amended after the signing of an antitrust settlement with the Federal Trade Commission ("FTC") in the United States.[33] Google claimed in its defense that the licensing clauses of the AdWords API were essential to combat the so-called "lowest common denominator problem." It maintained that if the input fields were standardized for online campaigns, Google AdWords' features would be curtailed and deprecated just for compatibility with other rival platforms.[34] The vote-reporter accepted that defense and considered that "if the software undermined the input fields for this full compatibility with the most varied platforms, advertisers could have access to less complete services, which could be detrimental to their experience with the products developed by the platforms."[35]

Another compelling investigation by CADE shows how limitations on interoperability can constitute antitrust law violations in the financial system. In 2019, CADE opened an investigation against a large Brazilian bank called Bradesco based on a complaint that the bank was preventing access to data by a firm that owns a smartphone app called Guiabolso.[36] In short, Guiabolso offers its users personal finance management tools and credit services within the app. Bradesco was accused of imposing technical difficulties for the bank's customers to access Guiabolso. Bradesco implemented a token system with random double-check passwords in its internet banking application. Since this double password verification system was not available for the Guiabolso application, Bradesco customers were often unable to access the functionality of that app.

The case was closed at CADE in 2020 with the signing of a settlement agreement. Bradesco committed to "develop connection interfaces that allow Guiabolso to (i) offer and capture the consent of its users who are also customers of Bradesco; and (ii) access Bradesco's systems, through previously established encrypted communication, allowing the collection of all data from users who provided consent."[37] Thus, Bradesco would have to develop technical functionalities allowing its customers to manifest their consent to use Guiabolso. While Bradesco would be allowed to use the password generator token, this token technology could not prevent contracting financial services with rival firms.

When the two cases are compared, some insights emerge about antitrust remedies. When imposing interoperability mandates, antitrust authorities sometimes feel compelled to decide which market factors will be left entirely to competition and which factors should be neutralized as preconditions for rivals to operate. This decision implicates much more than considering whether reactive and proactive antitrust remedies. It involves, after all, deciding what aspect of the design of digital products should be subject to market contestability.

In the Google case, CADE chose not to engage in the redesign of the input channels for AdWords API advertising campaigns. One can assert that, in essence, the authority held that this degree of intervention could adversely interfere with competition for API design. However, CADE could have engaged in more discussion on how preponderant the innovation competition was in that market.

On the other hand, in the Guiabolso case, it seems that the security restrictions imposed by Bradesco were not regarded as an autonomous market competition parameter, at least not in the exact terms of the product design developed by Bradesco. The notion that customers' safety could be guaranteed by other alternatives that were less harmful to competition seems to have played a decisive role in the case. This thinking though also pervades the product design evaluation from a competitive perspective.

32 Administrative Council for Economic Defense (CADE). Administrative Process nº 08700.005694/2013-19. Rapporteur vote of Commissioner Maurício Oscar Bandeira Maia (SEI no. 0628841), 2019.

33 GILBERT, R. J. U.S. Federal Trade Commission Investigation of Google Search (2013). *SSRN Electronic Journa*l, v. 1, n. 1, p. 2, 2017.

34 CADE, *supra* note 38, paragraphs 123-124.

35 CADE, *supra* note 38, paragraphs 125.

36 Administrative Council for Economic Defense (CADE). Administrative Process nº 08700.004201/2018-38. Nota Técnica n°17/2019/CGAA2/SGA1/SG/CADE (SEI no. 0591539).

37 Administrative Council for Economic Defense (CADE). Administrative Process nº 08700.004201/2018-38. Nota Técnica n° 22/2020/CGAA2/SG/CADE (SEI no. 0816090), paragraph 19.

IV. FINAL REMARKS

Assessing restrictions on data portability and interoperability as antitrust violations requires more than the categorical thinking that traditionally guides abuse of dominance. Depending on how these restrictions occur, they could be needlessly confused with exclusivity agreements, discriminatory practices, or refusals to deal. Putting the practices into these old boxes may be of little value to antitrust authorities.

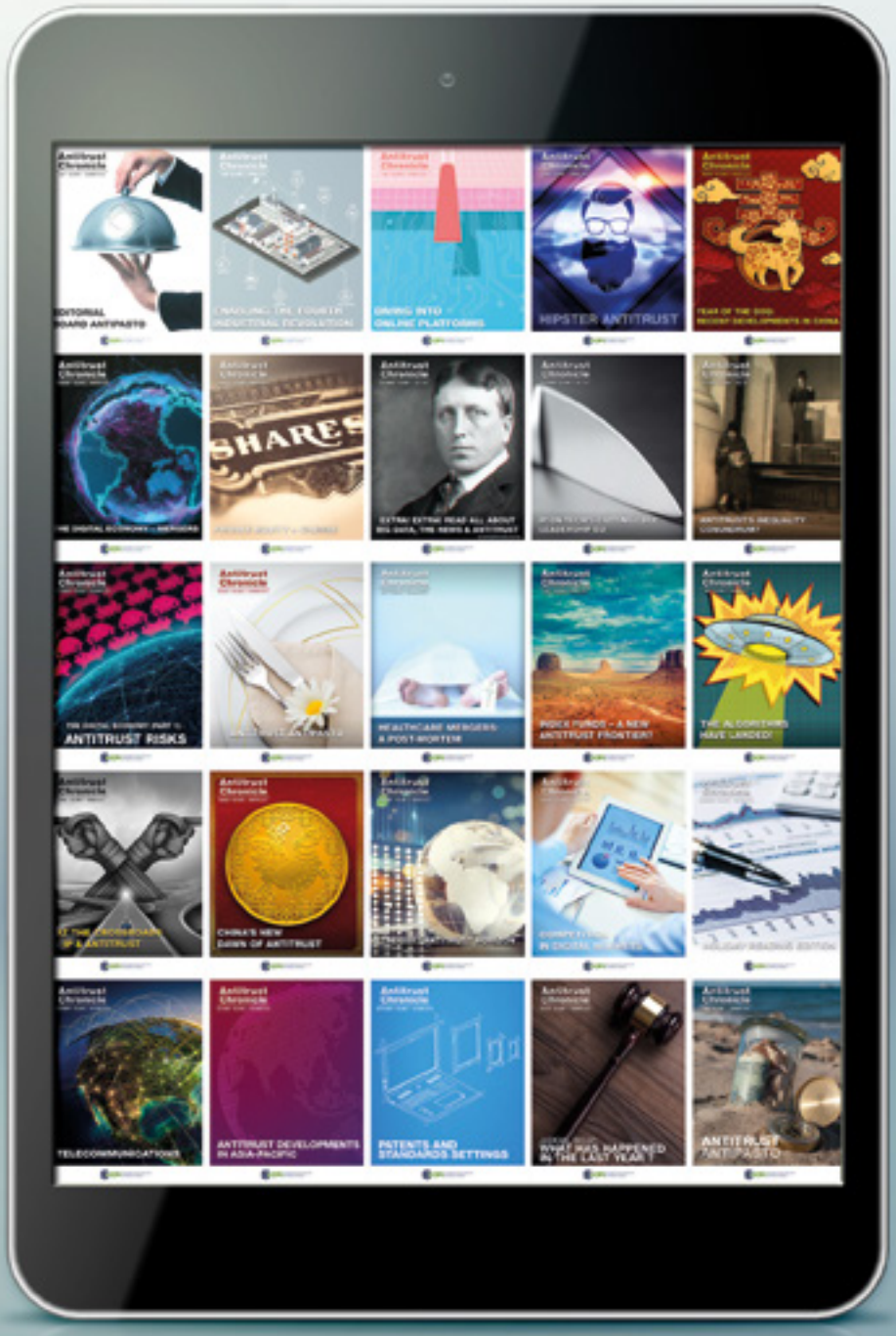
The real critical choices to be made by antitrust authorities when imposing remedies blur the limits of the intervention over the design of digital products. Agencies should be cautious in cases where enforcing interoperability is of little use in enhancing competition. However, when ease design solutions are available, condemning unilateral conducts may be a particularly interesting way to foster both competition and data protection goals in digital markets.

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

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




CPI
COMPETITION POLICY®
INTERNATIONAL