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.

CPI ANTITRUST CHRONICLE DECEMBER 2022

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.

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).

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.