

26 July 2021



CMA Mobile Ecosystems Market Study

DMG Media's submission on the Statement of Scope

1. DMG Media (which publishes the MailOnline, metro.co.uk and inews websites in the UK) welcomes the launch of the CMA's wide-ranging market study into mobile ecosystems and is keen to assist the CMA in its scoping and information gathering. In its view, the statement of scope published on 15 June 2021 is an excellent summary of the issues and DMG Media generally agrees with the workstreams proposed by the CMA.
2. This initial submission is divided in two parts. **Part I** focuses on the critical issues raised by "privacy washing" whereby Apple and Google weaponize privacy objectives to hand themselves insurmountable advantages over their competitors. Considering that the CMA has already investigated Google's conduct with respect to its Privacy Sandbox browser changes, we decided to focus on Apple's App Tracking Transparency ("ATT") policy change with respect to the Identifier for Advertisers ("IDFA"). ATT is a significant change brought into force by a digital gatekeeper without proper consultation and without regard for its profound consequences for the mobile ecosystem. It purports to improve user privacy, but its more significant result is to harm free-to-consumer apps that are paid for with advertising, such as MailOnline and other newspaper apps. In June 2021, MailOnline saw its average CPM (i.e., the price paid per 1,000 ad impressions) drop by [REDACTED] on iOS devices. Effects of this magnitude are significant for any business.¹ We use ATT as an opportunity to raise with the CMA issues of principle that in our view should be further explored in its market study. Apple and Google are acting as quasi-regulators for an entire industry, dictating what is acceptable from a privacy perspective and what is not. It is crucial that such power be subject to proper regulatory scrutiny and oversight to avoid unfair outcomes and distortions of competition. **Part II** discusses Apple News. Apple News is an important case study for Apple's use of privacy washing, in combination with other tactics such as the pre-installation of its own apps, to hand itself advantages in adjacent markets.

¹ These figures are worldwide figures. The available UK figures are less useful because they include MailOnline's direct sold ads, which add noise to the data. The UK effects are believed to be similar. We are happy to engage with the CMA to produce further data.

I. Privacy washing

3. The CMA has rightly included privacy washing issues in its statement of scope:
 - a. Google disabling third party cookies and Apple's ATT (mentioned at paragraphs 102, 123 and 133-134);
 - b. Google and Apple acting as quasi-regulators on privacy and user security issues (paragraph 103); and
 - c. Establishing the primacy of walled garden ecosystems to the detriment of the open web (paragraph 103).
4. We therefore hope that this will be one of the major themes in the market study.
5. As the CMA has been investigating Google for a couple of years now, first in the digital advertising market study and now in the Privacy Sandbox antitrust investigation, its knowledge of Google is already deep. This submission will focus primarily on Apple for which the CMA's analysis is perhaps less developed.
6. The CMA is rightly taking action to prevent the potential harm from Google's Privacy Sandbox proposals materialising in the first place.² In many ways, Apple's ATT raises similar types of issues, but its harmful effects will now need to be unravelled after the event. This is more difficult, but at least the CMA will be able to see data on the early effects of the policy change. We are hopeful that the CMA can act before the competitive landscape is harmed beyond repair. In what follows we first provide the background, discussing in-app advertising and the role of the IDFA (Section A). We then focus on the ATT solicitation and the effects that have been observed in the market as of today (Section B). We then show that while impairing effective digital advertising on iOS, Apple is expanding its own profitable advertising business (Section C). We use the example of the ATT solicitation as an opportunity to raise with the CMA some issues of principle with respect to Apple and Google's role as "quasi-regulators" that in our view should be further explored in its upcoming market study (Section D).

A. In-app advertising and the role of the IDFA

7. There are two basic models for a publisher to generate revenue to fund a mobile app. The publisher can charge a download fee and/or subscription fee to users, or it can offer the app for free and monetise its content by selling advertising space. Since many users are

² Competition and Markets Authority, Notice of intention to accept commitments proposed by Google in relation to its Privacy Sandbox Proposals, 11 June 2021, available at https://assets.publishing.service.gov.uk/media/60c21e54d3bf7f4bcc0652cd/Notice_of_intention_to_accept_binding_commitments_offered_by_Google_publication.pdf.

unwilling to pay for online (including news) content and would rather see ads, the ad-supported model is one of the primary methods by which publishers generate revenue.

8. For a publisher using an ad-supported business model, maximising the value of its advertising space (or “inventory”) is the lifeblood of its business. A publisher can fund an ad-supported app only if advertisers are willing to buy the publisher’s inventory. For an advertiser, a publisher’s inventory is substantially more valuable if it can access information about the user visiting the publisher’s content and measure the success of its campaign.
9. Mobile advertising is witnessing significant growth, with mobile ad spend reaching \$240 billion in 2020, and expected to top \$290 billion in 2021.³ The shift to mobile reflects the fact that consumers spend increasing amounts of time on their mobile devices (and apps in particular). According to App Annie, in Q1 2021, mobile users spent more than 4 hours in apps on average,⁴ while eMarketer found that in 2020 time spent with mobile increased by an average of 31 minutes per US adult, reaching 4 hours and 16 minutes.⁵
10. Much like web advertising, advertising on mobile apps (also referred to as “in-app advertising”) involves a variety of actors forming a complex ecosystem, most of which the CMA has examined as part of its seminal market study into digital advertising.⁶ The main actors are ad servers for publishers, ad servers for advertisers, SSPs (for Supply Side Platforms), ad networks, and DSPs (for Demand Side Platforms). For app campaigns an additional type of vendors are so-called Mobile Measurement Partners (“MMPs”), namely attribution providers which help marketers assess the effectiveness of their campaigns.⁷ A considerable proportion of in-app ads are so-called “app install ads,” namely ads that prompt the user to download an app (think of an ad on the MailOnline app promoting a new game app). App install ads are used by app developers for user acquisition, that is to expand their user base.

3 Lexi Sydow, “The State of Mobile in 2021: How to Win in a Mobile-Centric New Normal”, *App Annie*, 13 January 2021, available at <https://www.appannie.com/en/insights/market-data/state-of-mobile-2021/>.

4 Donny Kristianto, “Winning the Attention War: Consumers in Nine Major Markets Now Spend More than Four Hours a Day in Apps”, *App Annie*, 8 April 2021, available at <https://www.appannie.com/en/insights/market-data/q1-2021-market-index>.

5 Yoram Wurmser, “US Time Spent with Mobile 2021”, *eMarketer*, 2 June 2021, available at <https://www.emarketer.com/content/us-time-spent-with-mobile-2021>.

6 Competition and Markets Authority, Online platforms and digital advertising, Market study final report, 1 July 2020, available at https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TE_XT.pdf (the “CMA Final Report”).

7 Examples of MMPs include Adjust, AppsFlyer, Branch, Singular, and Kochava.

11. Advertising may be personalised (also referred to as “interest-based”) or not, depending on whether ads are targeted based on the interests of the audience or rather the content of the app.⁸ Personalised advertising promises marketers the ability to deliver the right message to the right user at the right time, thus reducing media waste and improving Return on Investment (“ROI”), while showing users ads that are more relevant to them. Importantly, personalised advertising brings significantly more revenue for publishers, allowing them to invest in new content that is offered to users for free. Replicating a trial originally conducted by Google, the CMA found that at least in the short term, removing third-party cookies leads to a 70% reduction in publisher revenue per page view.⁹ With respect to app advertising in particular, a study from Facebook shows that non-personalised advertising results in approximately 50% less publisher revenue.¹⁰
12. Whether personalised or not, for digital advertising to be effective, marketers must be able to measure the success of their advertising campaigns – and, in particular, measure whether the user “converted” (e.g., downloaded their app or performed an in-app event such as purchasing a subscription). Conversion measurement and attribution are necessary preconditions for effective online marketing, and they are used to optimize ad spend (e.g., the marketer may adjust its campaign in real-time to optimize towards conversions). In the case of in-app campaigns, attribution is typically performed by MMPs.¹¹
13. The ability to perform the functionalities mentioned above is largely dependent on the ability to track users. As the CMA has observed in its seminal market study and its investigation into Google’s Privacy Sandbox browser changes, user tracking serves a range of purposes in digital advertising, and in particular allows for (a) ad targeting, including interest-based targeting and retargeting; (b) measurement, attribution, frequency

8 See Competition and Markets Authority, Online platforms and digital advertising, Final Report, Appendix G: the role of tracking in digital advertising, available at https://assets.publishing.service.gov.uk/media/5efb1d6ae90e075c53dfce67/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential.pdf, paragraph 12(c): “Unlike contextual advertising, which relies on information about the content and context of the webpage or app that the user is currently viewing (such as keywords or topics), personalised advertising is concerned with knowing about an individual to determine whether to show them any ads, which ads to show them, and to measure their behaviour after they were exposed to the ad.”

9 Competition and Markets Authority, Online platforms and digital advertising, Final Report, Appendix F: the role of data in digital advertising, 1 July 2020, available at https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf, paragraphs 115-119.

10 Facebook for Developers, “The Value of Personalized Ads to a Thriving App Ecosystem”, 18 June 2020, available at <https://developers.facebook.com/blog/post/2020/06/18/value-of-personalized-ads-thriving-app-ecosystem>.

11 While marketers may also use each ad network’s attribution tools, this results in a fragmented approach and discrepancies, with each network reporting differently. An MMP helps the marketer to have a holistic view of its campaigns and perform accurate attribution across different networks. Typically, the marketer will integrate the MMPs Software Development Kit (“SDK”) in its app, so that the MMP may receive various data signals (user actions within the app).

capping, and reporting; and (c) spam and fraud detection.¹² This has led the CMA to explain that third-party cookies (which are the principal means of tracking users on the web) are a “fundamental building block of the open display advertising used by publishers and ad tech providers.”¹³

14. If third-party cookies are the backbone of open display advertising on the web, then mobile device advertising identifiers are the backbone of open display advertising on apps. Mobile device advertising identifiers – namely the IDFA for iOS and the Android Advertising ID for Android – are the equivalent of third-party cookies in the app ecosystem, and serve a range of advertising purposes, including measurement/attribution, frequency capping, and targeting.
15. The IDFA is a random string of alphanumerical characters assigned by the OS to pseudonymously identify a user’s device, exclusively for advertising purposes.¹⁴ It was first introduced by Apple in 2012 to replace identifiers which were used for advertising purposes, but which could not be disabled or reset by the user.¹⁵ The IDFA may be manually reset by the user or disabled altogether through the “Limit Ad Tracking” (“LAT”) option in the iPhone’s settings. Since iOS 10, when a user enables the LAT option, Apple sends a string of zeros in place of the IDFA.¹⁶ In 2020, almost 28% of iOS users in the UK had enabled LAT.¹⁷ LAT applies equally to apps from Apple (e.g., Apple News) and third-party apps (e.g., MailOnline).

12 Competition and Markets Authority, Notice of intention to accept commitments proposed by Google in relation to its Privacy Sandbox Proposals (Case number 50972), 11 June 2021, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/992975/Notice_of_intention_to_accept_binding_commitments_offered_by_Google_publication.pdf, paragraph 5.10. See also paragraph 5.30 (expressing the competition concern that the Privacy Sandbox Proposals, if implemented without regulatory oversight, would limit functionalities associated with user tracking, thus having a negative impact on the ability of publishers to sell ad inventory in competition with Google).

13 Id., paragraph 5.32; CMA Final Report, paragraph 5.323.

14 The Apple Developer License Program Agreement provides at Section 3.3.12 that “You and Your Applications (and any third party with whom You have contracted to serve advertising) may use the Advertising Identifier, and any information obtained through the use of the Advertising Identifier, only for the purpose of serving advertising.”

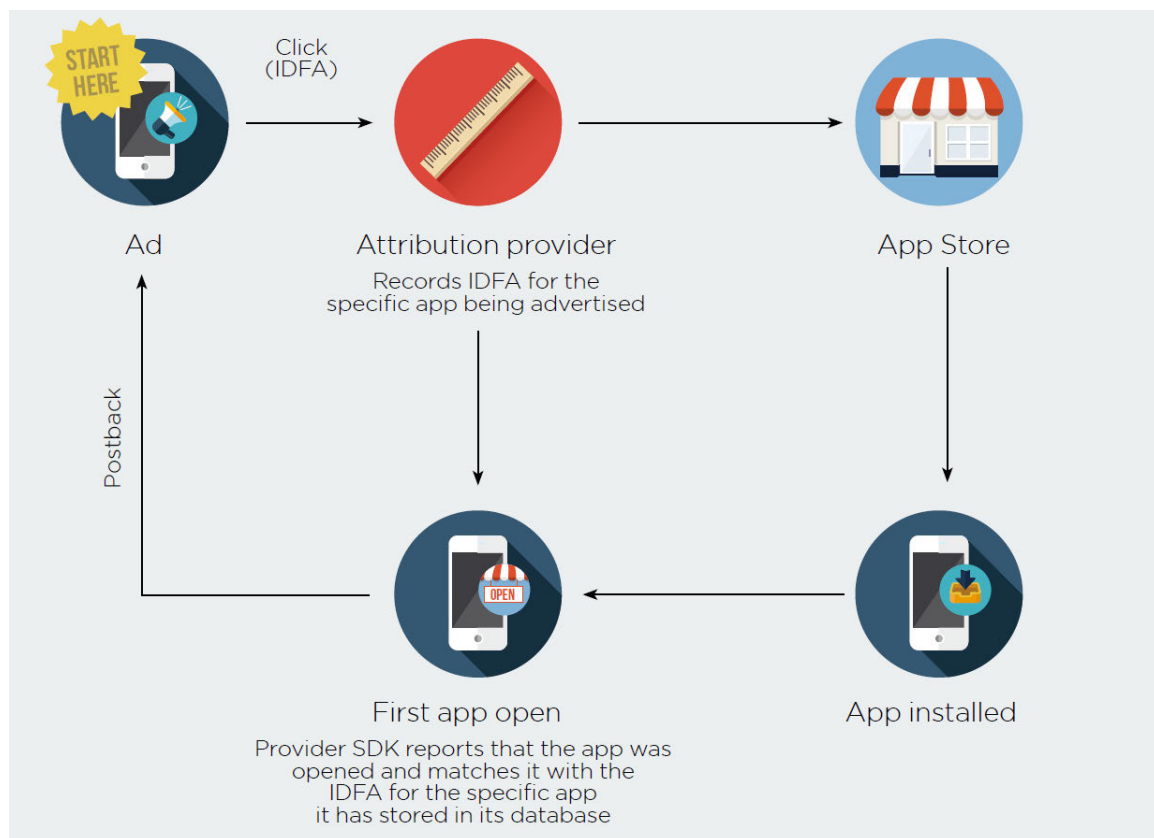
15 Sarah Perez, “iOS 7 Eliminates MAC Address As Tracking Option, Signaling Final Push Towards Apple’s Own Ad Identifier Technology”, *TechCrunch*, 14 June 2013, available at <https://techcrunch.com/2013/06/14/ios-7-eliminates-mac-address-as-tracking-option-signaling-final-push-towards-apples-own-ad-identifier-technology/>.

16 Before iOS 10, when users actively selected LAT, the operating system would send a “flag” indicating that the user has chosen to limit ad tracking. See Ziv Bass Spektor, “FAQ: Impact of Apple (iOS) Limit Ad Tracking on attribution”, *AppsFlyer*, 13 September 2020, available at <https://support.appsflyer.com/hc-en-us/articles/115003734626-FAQ-Impact-of-Apple-iOS-Limit-Ad-Tracking-on-attribution>.

17 John Koetsier, “Privacy checkup: Limit Ad Tracking up 216% on iOS, but down 85% on Android”, *Singular Blog*, 27 March 2020, available at <https://www.singular.net/blog/limit-ad-tracking-privacy-checkup-in-2020/>.

16. To illustrate the importance of the IDFA, consider the following example. A user downloads a game app (say Candy Crush Saga). The latter would like to determine whether that download is organic or rather the outcome of its marketing campaigns across various sources (which may include app install ads on the MailOnline app). To this end, the game app will typically rely on its MMP (whose SDK will be integrated in its app). Once the user opens the game app, the MMP will read the IDFA (subject to privacy legislation requirements) and match it with the IDFA of any user that clicked on the app install ads shown on various apps (including the MailOnline app) to attribute the download.¹⁸ This process is illustrated in Figure 1 below.

Figure 1 (source: AppsFlyer)



17. MailOnline accesses the user's IDFA in full compliance with the applicable privacy legislation – in the UK, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations. In practice, wherever the user has not provided consent, MailOnline does not access the IDFA.¹⁹

¹⁸ MMPs are typically called when a user clicks on an ad so they can store the user's IDFA.

¹⁹ App developers are also contractually obliged by Apple to protect user privacy and comply with all applicable laws, on pain of being removed from the App Store and the Apple Developer Program. See App Store Review Guidelines, available at <https://developer.apple.com/app-store/review/guidelines/> (last

B. The ATT solicitation – effects as of today

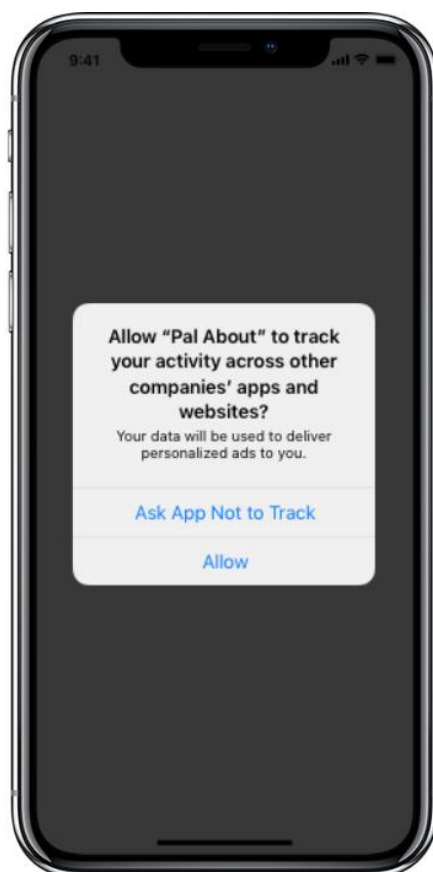
1. The ATT solicitation

18. In June 2020, Apple announced that in the future app developers (and their ad tech partners) would be able to access the IDFA or “track” the user (as defined by Apple) only if the user granted permission through an Apple-designed pop-up, purportedly to increase user privacy. The developer may call the ATT solicitation upon app launch or at a later stage, but in any event before it can access the IDFA or track the user.²⁰ Originally slated for release in September 2020 as part of iOS 14, the ATT solicitation was eventually introduced on 26 April 2021 alongside iOS 14.5. See Figure 2 below for an example of the ATT solicitation.

accessed on 19 July 2021), Section 5.1 and in particular 5.1.1 (stating that apps must include a link to their privacy policy in the App Store Connect metadata field and within the app; stating that apps collecting user or usage data must secure user consent or pursue a legitimate interest according to the requirements of the GDPR) and 5.1.2 (stating that unless otherwise permitted by law, using or sharing personal data requires first permission, and that data collected from apps may only be shared with third parties to improve the app or serve advertising in line with the Apple Developer Program License Agreement; explaining that apps that share user data without user consent or otherwise complying with data privacy laws “may be removed from sale and may result in your removal from the Apple Developer Program”).

20 “Details for app privacy questions now available”, Apple Developer, 3 September 2020, available at <https://developer.apple.com/news/?id=hx9s63c5>. See “User Privacy and Data Use”, App Developer, available at <https://developer.apple.com/app-store/user-privacy-and-data-use/>.

Figure 2 (source: Apple)



19. If the user taps “Allow”, the app may access the IDFA and “track” the user (as defined by Apple). If the user taps “Ask App Not to Track”, Apple sets the IDFA’s value to a string of zeros (so that it cannot be used to identify the user), and the app developer is prohibited from tracking the user.²¹ This is regardless of whether the developer has already obtained consent e.g., for personalized advertising, in compliance with the applicable privacy legislation; the choice in the ATT solicitation overrides any other choice.²²

21 “User Privacy and Data Use”, App Developer, available at <https://developer.apple.com/app-store/user-privacy-and-data-use/>. Note that LAT as a setting will continue to exist at the device level. Thus, if a user has the LAT option turned on, no app will have access to the IDFA. See Eric Benjamin Seufert, “Apple killed the IDFA: A comprehensive guide to the future of mobile marketing”, *Mobile Dev Memo*, 29 June 2020, available at <https://mobiledevmemo.com/mobile-advertising-without-the-idfa-a-comprehensive-overview/>.

22 See “User Privacy and Data Use”, App Developer, available at <https://developer.apple.com/app-store/user-privacy-and-data-use/>, last accessed on 12 July 2021: “[Question:] Can I add other permission requests in order to comply with regulations, such as ePrivacy or GDPR? [Answer:] Yes, you can choose to include screens in order to comply with government regulations. However, your app must always respect the user’s response to the AppTrackingTransparency prompt, even if their response to other prompts conflicts.”

20. “Tracking” is defined (broadly) by Apple as the “act of linking user or device data collected from [an] 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.”²³ As noted above, “tracking” covers a variety of use cases, ranging from the provision of personalised advertising to frequency capping and measurement / attribution.
21. The design of the box and the message displayed to the user are prescribed by Apple; developers are only allowed to customise the non-bolded text (which in Figure 2 above reads “*Your data will be used to deliver personalized ads to you.*”). As a result, all users are served with the ominous warning that the app would like to “*track you across apps and websites owned by other companies.*”
22. Apple has made it clear that unless the user taps “Allow,” the developer and its ad tech vendors are prohibited from using alternative methods not relying on the IDFA to track the user, such as hashed email address or phone number or fingerprinting.²⁴ Importantly, Apple updated its App Store Review Guidelines to prohibit app developers from incentivising users to allow tracking or from denying access to the app (“gating functionality”) to users that do not grant permission.²⁵

-
- 23 “User Privacy and Data Use”, App Developer, available at <https://developer.apple.com/app-store/user-privacy-and-data-use/>, last accessed on 12 July 2021. Thus, developers will have to get user permission in order to, inter alia, display targeted advertisements in their app based on user data collected from apps and websites owned by other companies; share device location data or email lists with a data broker; share email lists, advertising IDs, or other IDs with a third-party advertising network for retargeting; place a third-party SDK in their app that combines user data across apps to target advertising or measure advertising efficiency, even if the app developer itself does not use the SDK for these purposes (but e.g., an analytics SDK repurposes the data it collects from the app on which it is placed to enable targeted advertising in other developers’ apps). On the contrary, user permission is not required “[w]hen user or device data from your app is linked to third-party data solely on the user’s device and is not sent off the device in a way that can identify the user or device; When the data broker with whom you share data uses the data solely for fraud detection, fraud prevention, or security purposes, and solely on your behalf. For example, using a data broker solely to prevent credit card fraud.”
- 24 “User Privacy and Data Use, App Developer, available at <https://developer.apple.com/app-store/user-privacy-and-data-use/>, last accessed on 12 July 2021: “[Question:] If I have not received permission from a user via the tracking permission prompt, can I use an identifier other than the IDFA (for example, a hashed email address or hashed phone number) to track that user? [Answer:] No. You will need to receive the user’s permission through the AppTrackingTransparency framework to track that user. [...] [Question:] Can I fingerprint or use signals from the device to try to identify the device or a user? [Answer:] No. Per the Apple Developer Program License Agreement, you may not derive data from a device for the purpose of uniquely identifying it.”
- 25 “User Privacy and Data Use, App Developer, available at <https://developer.apple.com/app-store/user-privacy-and-data-use/>, last accessed on 12 July 2021: “[Question:] Can I gate functionality on agreeing to allow tracking, or incentivize users to agree to allow tracking in the app tracking transparency prompt? [Answer:] No, per the App Store Review Guidelines: 3.2.2 (vi).” Section 3.2.2.(vi) of the App Store Review Guidelines provides that “Apps should not require users to rate the app, review the app, watch videos, download other apps, tap on advertisements, enable tracking, or take other similar actions in order to access functionality, content, use the app, or receive monetary or other compensation, including but not limited to gift cards and codes.”

23. In addition, iOS 14.5 incorporates a prominent “Tracking” section in its Privacy Settings (seen in Figure 3), where users are able to fully block requests by third-party apps to be tracked.²⁶ This replaces the LAT option which could be found up until iOS 13, and effectively allows the user to prevent tracking altogether.

Figure 3 (source: 9to5Mac)



2. Effects observed as of today

24. In the period between Apple’s announcement of the ATT framework and the latter’s official rollout, several commentators warned that Apple’s policy change would throw the entire industry in disarray.²⁷ While Apple would not deprecate the IDFA, in practice the result would be the same for most cases, since very few users were expected to opt in. Considering the language in the pop-up, and the fact that there is no downside to tapping “Ask App Not To Track,” industry analysts were expecting a user opt-in rate ranging between 1% and 20%, implying that the IDFA would no longer be available for the majority of users.²⁸ Since the IDFA is the backbone of effective advertising on apps,

²⁶ The default will be to allow apps to ask users permission to track them.

²⁷ See e.g., John Koetsier, “Apple Killed The IDFA. What Else Dies?”, *Forbes*, 29 June 2020, available at <https://www.forbes.com/sites/johnkoetsier/2020/06/29/apple-killed-the-idfa-what-else-dies/>.

²⁸ See e.g., Michael Sweeney, “Apple’s Changes to IDFA in iOS 14: FAQs and the Impact on Mobile Advertising”, *The Clearcode Blog*, available at <https://clearcode.cc/blog/apple-idfa/#opt-in>; Eric Benjamin Seufert, “Apple killed the IDFA: A comprehensive guide to the future of mobile marketing”, *Mobile Dev Memo*, 29 June 2020, available at <https://mobiledevmemo.com/mobile-advertising-without-the-idfa-a-comprehensive-overview/>; Allisson Schiff, “Will People Actually Opt In To IDFA Tracking?”,

Apple's policy change was thus expected to negatively impact publisher's ability to generate advertising revenue,²⁹ as well as marketers' ability to accurately measure campaigns. Early evidence seems to confirm these predictions.

25. While officially launched in April 2021, it was not until last month that the first effects of Apple's policy change were felt, as a result of the comparatively slow penetration rate of iOS 14.5.³⁰ However, as of late June more than 75% of iOS devices have upgraded to an iOS version that requires apps to use the ATT to access IDFA.³¹ Current analyses show that the opt-in rate does not exceed 30% in the EEA, and 23.2% in the UK.³² This is consistent with MailOnline's experience. Since the release of iOS 14.5, MailOnline's access to the IDFA has kept decreasing as more iOS users installed the software update on their phone. Between 1 May 2021 and 6 July 2021, the opt-in rate for all iOS users has decreased from [REDACTED] to [REDACTED]. As devices continue to upgrade to iOS 14.5, it is likely to continue to fall: around [REDACTED] of MailOnline's traffic is now on iOS 14.5 versions or succeeding versions. In practice, however, the actual rate is very likely much lower, since for use cases such as conversion measurement / attribution the user has to opt in *twice*, both when using the app of the advertiser (where the conversion happens) and when using the app of the publisher (where the ad is shown).³³ An analyst from Branch thus found that the attribution rate is 7% of the pre-ATT baseline.³⁴

AdExchanger, 25 June 2020, available at <https://www.adexchanger.com/mobile/will-people-actually-opt-in-to-idfa-tracking/>; John Koetsier, "Apple Just Crippled IDFA, Sending An \$80 Billion Industry Into Upheaval", *Forbes*, 24 June 2020, available at <https://www.forbes.com/sites/johnkoetsier/2020/06/24/apple-just-made-idfa-opt-in-sending-an-80-billion-industry-into-upheaval/>.

- 29 Lukas I. Alpert and Patience Haggin, "Publishers Brace for Impact From Apple's New Privacy Controls", *The Wall Street Journal*, 27 August 2020, available at <https://www.wsj.com/articles/publishers-brace-for-impact-from-apples-new-privacy-controls-11598565920>.
- 30 As of May 27, 2021, the penetration rate of iOS 14.5 had been very low. See <https://twitter.com/alexdbauer/status/1398063654688284676> for an illustrative graph comparing penetration rates of iOS versions.
- 31 <https://twitter.com/alexdbauer/status/1410073980283748355>.
- 32 John Koestier, "SKAdNetwork impact: Android ad spend, ATT opt-in rates, ad network growth, and iOS 14.5 adoption", *Singular*, 6 July 2021, available at: <https://www.singular.net/blog/skadnetwork-ios145-adspend/>. See also Kurt Wagner, Facebook Users Said No to Tracking. Now Advertisers are Panicking, *Bloomberg*, 14 July 2021, available at <https://www.bloomberg.com/news/articles/2021-07-14/facebook-fb-advertisers-impacted-by-apple-aapl-privacy-ios-14-changes>, explaining that Branch has found that people give permission only 25% of the time.
- 33 See e.g., John Koetsier, "Apple's iOS 14.5 Boosted A Key Android App Profitability Factor By 2.5X", *Forbes*, 25 June 2021, available at <https://www.forbes.com/sites/johnkoetsier/2021/06/25/apples-ios-145-boosted-a-key-android-app-profitability-factor-by-25x/?sh=38fbbc444132> (noting that double permission is required, to the effect that "full trackability a la 2010 to 2020 is only available for a vanishingly small percentage of their mobile users.") See also Ari Paparo, "IDFA Apocalypse: What We Know (And Don't)", *AdExchanger*, 14 July 2020, available at <https://www.adexchanger.com/data-driven-thinking/idfa-apocalypse-what-we-know-and-dont/>.
- 34 See <https://twitter.com/alexdbauer/status/1410073998629638150/photo/1>.

26. Consistent with the low numbers of opt-in rate, iOS apps have witnessed a significant drop in their advertising revenue. According to ad measurement firm Tenjin, in June 2021 ad spend on iOS dropped by around one-third.³⁵ MailOnline is still monitoring the performance of its inventory, but the results so far are discouraging. MailOnline's average CPM for iOS supply before the rollout of the ATT was around \$[REDACTED] while its average CPM since the implementation of the ATT is \$[REDACTED].³⁶ This amounts to a [REDACTED] decrease. This comes at a time when news publishers find it harder and harder to sustain their ad-funded business model, partly because the majority of digital ad spend is captured by the walled gardens of Google and Facebook, and partly because tracking restrictions in the most popular browsers (already Safari and soon Chrome) reduce the prices for web inventory.³⁷ We encourage the CMA to use its information-gathering powers within the context of its market study to gather additional evidence on the precise effects of Apple's policy change on publishers' ad revenue.

27. As noted above, the negative effects of Apple's policy change were expected. By (practically) removing the IDFA in most cases without offering any effective alternative in place, Apple has impaired the effectiveness of digital advertising on iOS devices. The only "alternative" Apple has offered is the SKAdNetwork attribution solution, which however suffers from considerable limitations.

28. First launched in 2018,³⁸ the SKAdNetwork is in practice the *de facto* way to attribute app installs in the absence of IDFAs.³⁹ At the heart of the SKAdNetwork architecture lies no one else than Apple itself, as it is the entity that performs attribution (through the App Store) by matching app installs and campaigns. Besides Apple, the parties involved are (a) the ad network (the vendor delivering the ad and driving app installs and conversions); (b) the source app (the publisher); and (c) the advertised app.⁴⁰ Under the SKAdNetwork, once the user downloads an app, Apple performs attribution and sends a postback to the ad network that drove the install. The postback includes limited information, and does not

35 <https://blog.tenjin.com/ios-15-new-challenges/>. Note that ad spend on Android saw an increase of about 10%.

36 Data refers to effective CPM ("eCPM"), which takes into account the CPM paid and the fill rate.

37 Google recently announced that it is delaying its deprecation of tracking cookies, following its offer of commitments to the Competition and Markets Authority. See Oliver Bethell, "Our commitments for the Privacy Sandbox", *The Keyword*, 11 June 2021, available at <https://blog.google/around-the-globe/google-europe/our-commitments-privacy-sandbox/>.

38 At the time SKAdNetwork went largely unnoticed due to its limitations compared to rival solutions. See e.g., Barak Witkowski, "What Is SKAdNetwork?", *AdMonsters*, 9 September 2020, available at <https://www.admonsters.com/what-is-skadnetwork/>.

39 Allisson Schiff, "Apple's SKAdNetwork Gets Real – Is It The Future Of Mobile App Attribution On IOS?", *AdExchanger*, 7 July 2020, available at <https://www.adexchanger.com/mobile/apples-skadnetwork-gets-real-is-it-the-future-of-mobile-app-attribution-on-ios/>.

40 "Apple's SKAdNetwork Explained", *Ad Tech Explained*, 22 August 2020, available at <https://adtechexplained.com/skadnetwork-explained/>.

contain any user-level data.⁴¹ Apple sends the postback to the ad network on the basis of a complicated sequence of timers, which in practice means that postbacks could be delayed anywhere from 24 hours to around 63 days.⁴²

29. SKAdNetwork suffers from several limitations compared to existing methods of attribution. It does not support user-level attribution; instead, attribution is done at an aggregate level. SKAdNetwork lacks in the granularity of events that are reported back to the ad network. Second, the postback is sent with significant delay (24 hours is the minimum), i.e. there is no real-time data provided to the ad network, which makes campaign optimisation in real-time (“on the fly”) impossible. These limitations represent a loss of efficiency for marketers – and in turn a loss of revenue for publishers, since marketers are not willing to spend their budgets buying media which cannot be accurately measured and against which they cannot optimise their bidding strategies.

30. SKAdNetwork also means that Apple will get to grade the homework for everyone, as it will be the entity matching app installs and campaigns. Accurate independent attribution will thus be limited to the very small number of cases where the IDFA is present.

C. While impairing effective digital advertising on iOS, Apple is expanding its own profitable advertising business

31. While impairing effective digital advertising on iOS, Apple is at the same time expanding its own profitable advertising business, estimated at \$ 2 billion for 2020,⁴³ and which will remain unaffected by the ATT policy change. The reason is that Apple subjects iOS users to personalized advertising *by default*, that is without obtaining opt-in user consent (see Figures 4 and 5 below). Users must, therefore, first realise that Apple engages in personalised advertising and, then, find out how to opt-out by navigating the iPhone’s settings.⁴⁴

41 The information in the postback includes: the ad network ID (used to identify the particular ad network), the ID of the source app (used to identify the publisher where the ad appeared), the ID of the advertised app (used to identify the marketer), a value indicating whether the app install was a re-download or not, the campaign ID (limited to 100 values; may be used to indicate any other campaign information such as creative and placement), a conversion value (a number between 0 and 63 which can be used to indicate a conversion event), and Apple’s cryptographic signature (which the ad network uses to verify the postback).

42 For a technical explanation, see “How does the conversion value timer logic work in SKAdNetwork?”, *Quantmar*, available at <https://quantmar.com/715/How-does-the-conversion-value-timer-logic-work-skadnetwork>.

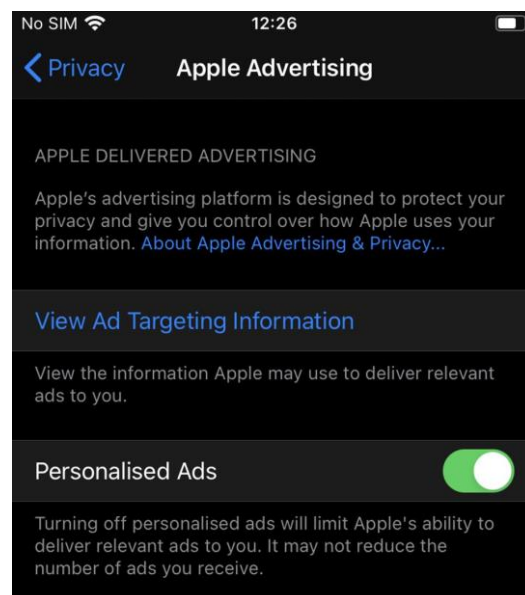
43 See Amy Gesenhues, “Apple search ads expected to generate \$2 billion in revenue by 2020”, *Search Engine Land*, 22 October 2018, available at <https://searchengineland.com/apple-search-ads-expected-to-generate-2-billion-in-revenue-by-2020-306882>.

44 Patience Haggin and Jeff Horwitz, “Facebook Says Apple’s New iPhone Update Will Disrupt Online Advertising”, *The Wall Street Journal*, 26 August 2020, available at

Figure 4 (source: Technology Magazine)



Figure 5 (source: Forbes)



<https://www.wsj.com/articles/facebook-says-apples-new-iphone-update-will-disrupt-online-advertising-11598458715>; Anthony Ha, Matthew Panzarino, "Apple's App Tracking Transparency feature will be enabled by default and arrive in 'early spring' on iOS", TechCrunch, 28 January 2021, available at: <https://techcrunch.com/2021/01/27/apple-app-tracking-transparency/>.

32. But even when users do find the setting, Apple’s language is designed to minimise the chances of them opting out: “*Apple advertising platform is designed to protect your privacy and give you control over how Apple uses your information.*” [...] *Turning off personalised ads will limit Apple’s ability to deliver relevant ads to you. It may not reduce the number of ads you receive.*”
33. This form of self-preferencing is not limited to choice architecture and defaults though. Apple has also introduced features to privilege its own ad network in the form of additional reporting data compared to that available to users of SKAdNetwork.⁴⁵ Against that background, Apple’s recent introduction of a new ad slot in the App Store – at the very moment the ATT policy change was rolled out – came as little surprise.⁴⁶ Apple’s continuous hiring of digital advertising experts – including former Facebook ads manager Antonio Garcia Martinez – is indicative of its future intentions.⁴⁷ As of May 10, Apple had about 50 open roles related to ad platforms.⁴⁸

D. Issues of principle raised by the ATT solicitation

34. We would like to use the ATT solicitation as an opportunity to raise with the CMA certain issues of principle which in our view should be further explored in the market study.
35. The ATT solicitation is not an isolated event – it is one of a series of unilateral actions of Apple and Google to restrict functionalities associated with digital advertising in the name of user privacy.⁴⁹ Typically, Apple will make the first move, using its gatekeeper position as a provider of a web browser (Safari) or mobile OS (iOS), all while presenting itself as the champion of consumer privacy. Google will then follow in Apple’s footsteps and roll

45 Eric Benjamin Seufert, “Apple privileges its own ad network with ATT. What’s its privacy endgame?”, *Mobile Dev Memo*, 1 February 2021, available at <https://mobiledevmemo.com/apple-privileges-its-own-ad-network-whats-its-privacy-end-game/>, explaining that “advertisers get more granular data about the campaigns they operate on Apple’s own ad network than they do for those run on any other network (eg. Facebook). This potentially makes it easier to optimize — and spend more money on — Apple ad network campaigns than campaigns run on other platforms.”

46 See Sarah Perez, “Apple expands its ad business with a new App Store ad slot”, *TechCrunch*, 5 May 2021, available at <https://techcrunch.com/2021/05/05/apple-expands-its-ad-business-with-a-new-app-store-ad-slot/>.

47 See Mike Peterson, “Apple hires Facebook ads manager, 'Chaos Monkeys' author Antonio Garcia Martinez”, *Apple Insider*, 10 May 2021, available at <https://appleinsider.com/articles/21/05/10/apple-hires-facebook-ads-manager-chaos-monkeys-author-antonio-garcia-martinez>. Antonio Garcia Martinez eventually resigned after internal protests within Apple.

48 Ibid

49 For Apple justifying ATT on privacy grounds, see e.g., Tim Cook’s response to Questions for the Record from the Honorable Ken Buck, added on 14 September 2020, available at <https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-20200729-QFR056.pdf>, page 1.

out similar changes, typically a couple of years later. We have seen that happen with respect to web advertising – where Apple’s Safari blocks third-party cookies by default, and now Google is planning on replacing third-party cookies on Chrome with its Privacy Sandbox browser changes – and we are expecting the same for app advertising (where Google has already announced it will tighten its Limit Ad Tracking feature for the Android Advertising ID).⁵⁰ As of lately, Apple has announced new features to obfuscate IP addresses (Private Relay) and randomize email addresses (Hide My Email) which will create new frictions in digital advertising in the name of user privacy⁵¹ – all while placing Apple in a unique position of strength.⁵² We would not be surprised if in a couple of years from now Google were to introduce similar features, for instance within the context of its Privacy Sandbox project.⁵³

36. There is now a clear pattern, with Apple taking unilateral actions to impair effective advertising in the name of privacy and then Google following suit at a later stage, pointing to Apple as an example. In effect, Apple is A/B-testing for Google. Yet we find it most problematic that essentially just two companies in the world – Apple and Google – get to set the rules and dictate what is acceptable or not from a privacy perspective for an entire industry. By owning the key digital access points (bottlenecks) – namely the two most popular browsers and smart mobile OSs – these companies control both consumers’ access to online content and business users’ access to consumers. This an unprecedented form of power in the digital economy – power which will rise in significance as we move further into the digital era. These companies act as *quasi-regulators*, setting and enforcing the rules on privacy as they deem fit – they are judge, jury, and executioner.
37. Such power needs to be subject to *regulatory oversight and scrutiny*, considering its potential for abuse and negative impact on bystanders. This is a matter of basic accountability and fairness. At the very least, these companies should not be able to

50 See James Hercher, Google Tightens ‘Limit Ad Tracking’ Policies For Android Ad ID, *AdExchanger*, 2 June 2021, available at <https://www.adexchanger.com/mobile/google-tightens-limit-ad-tracking-policies-for-android-ad-id/> (noting that “these updates to Android and the Google Play Store do follow in Apple’s pre-ATT footsteps”).

51 For instance, features randomizing email addresses could impair the effectiveness of digital advertising solutions relying on hashed email addresses.

52 On Private Relay, see for example Eric Benjamin Seufert, “It’s Apple’s internet now”, *Mobile Dev Memo*, 14 June 2021, available at <https://mobiledevmemo.com/its-apples-internet-now/> (explaining that “Apple is essentially positioning itself between a user and the internet as a gatekeeper. Right now, Private Relay merely masks the IP address of a device. But ultimately, Private Relay could moderate a device’s access to the internet in any number of ways. [...] the fact that many non-fingerprinting, legitimate uses of the IP address for websites will break with Private Relay, puts a premium on app-based content delivery. Publishers are better served with apps than mobile websites as a result of Private Relay.”)

53 Note that Google has already declared its hostility towards digital advertising solutions based on hashed email addresses. See David Temkin, “Charting a course towards a more privacy-first web”, *Google Ads & Commerce Blog*, 3 March 2021, available at <https://blog.google/products/ads-commerce/a-more-privacy-first-web/>.

implement drastic changes that affect entire industries without a form of *meaningful consultation* where affected stakeholders can be heard and influence the outcome. As of today, Apple has been left entirely free to proceed as it wishes, with limited to no constraints in its conduct. This needs to change. The CMA has already set an important precedent in that direction with its investigation into Google’s Privacy Sandbox browser changes and its synthetic approach towards privacy *and* competition; privacy is important and must be protected, but it cannot be the trump card that indiscriminately prevails over any other consideration, nor an excuse to distort competition or exploit customers.

38. The need for regulatory oversight is made even more compelling by the fact that Apple and Google are not neutral operators, nor charitable institutions. The policy changes they make in the name of user privacy will often benefit them at the expense of their competitors or customers. Take ATT for example. Apple has an *incentive* to impair the effectiveness of digital advertising on iOS, as this pushes developers to adopt a freemium model – in which case Apple conveniently gets a 30% commission.⁵⁴ At the same time, Apple is building its *own profitable advertising business on iOS*, which will remain unaffected by the ATT solicitation, since it subjects users to personalized advertising by default.
39. A related point is that Apple and Google have a very *specific* understanding of privacy – one that happens to be convenient to their own business. By referring to “tracking,” these companies draw a distinction between “first party data” (which is acceptable from a privacy standpoint) and “third party data” (which is not).⁵⁵ Yet this is a self-serving distinction not found anywhere else (e.g., legislation), which eventually incentivizes consolidation of data into single entities.
40. On closer inspection, Apple’s privacy credentials are in fact less impressive than what one might initially think. For one, Apple is happy to share Google’s advertising revenue realised on iPhones. Apple is reportedly paid by Google between \$ 8-12 billion per year

54 See Steve Latham, “Why Apple’s anti-tracking move hurts everyone ... but Apple”, *VentureBeat*, 12 September 2020, available at <https://venturebeat.com/2020/09/12/why-apples-anti-tracking-move-hurts-everyone-but-apple/> (“Of the 2.2 million apps in the Apple store, many will fail as ad revenue nosedives. Apps that are able to migrate to subscription models will pay a high price. Aside from the costly development work and the inevitable loss of users, publishers will have to pay Apple a 30% tax on new subscription revenue.”)

55 See Eric Benjamin Seufert, “The privacy mirage”, *Mobile Dev Memo*, 8 March 2021, available at <https://mobiledevmemo.com/the-privacy-mirage/> noting that “The false dichotomy that is being presented with mechanics like AppTrackingTransparency — in which privacy control options are packaged as delivering either total surveillance or total anonymity — doesn’t accurately describe the privacy reality of what the platforms are proposing to users. [...] If a user wants total anonymity, then using first-party data for ads targeting doesn’t accommodate that: if platforms want to offer a binary privacy choice, then they need to offer a “do not use any of my data to target or personalize ads” option, which they are not doing when they only use their own first-party data to target ads.”

for having Google Search as the default on Safari.⁵⁶ Worse, it is not even clear that Apple complies with the applicable privacy legislation with respect to its own advertising practices on iOS, since, as mentioned above, iOS users are subject to Apple’s personalised advertising by default. Apple’s default advertising settings are currently investigated by the French Data Protection Authority CNIL, following a complaint from the France Digitale association.⁵⁷

41. It should be noted that Apple targets users based on personally identifiable information, as it uses account information such as name, age and even address to assign the user to a segment and serve personalised advertising.⁵⁸ Apple may also assign the user to segments based on “[t]he music, movies, books, TV shows, and apps [she] download[s], as well as any in-app purchases and subscriptions,” and there is no sign in its policy that such data is derived only from the use of Apple’s own apps.⁵⁹ This means that Apple may assign users to segments based on their use of third-party apps and in-app purchases.

II. Apple News

42. Theme 4 in the CMA’s statement of scope does not explicitly mention Apple News, but it is a perfect example of the problem that Theme 4 is designed to investigate, i.e. Apple’s dual role as upstream app store gatekeeper and owner of the operating system and downstream competitor against other app developers and news services.
43. Apple operates a “freemium” model for its news service. Apple News is free to users, and it is pre-installed on iPhones and iPads. It is integrated into its operating system and can be accessed without clicking from the home screen because users just need to swipe right to access it. Users get notifications of news stories by default. Apple News+ is the subscription service, which users are frequently nudged to sign up for. It costs £9.99 per month in the UK.

56 Daisuke Wakabayashi and Jack Nicas, “Apple, Google and a Deal That Controls the Internet”, *The New York Times*, 25 October 2020, available at <https://www.nytimes.com/2020/10/25/technology/apple-google-search-antitrust.html>.

57 See Aoife White, Helene Fouquet and Stephanie Bodoni, “Apple Faces Next Round in French Probe Into iOS 14 Overhaul”, *Bloomberg*, available at <https://www.bloomberg.com/news/articles/2021-03-16/apple-s-ad-tool-faces-initial-probe-from-french-privacy-watchdog>.

58 See Apple Advertising & Privacy, available at <https://support.apple.com/en-us/HT205223>.

59 Ibid. The only limitation is that Apple does not allow targeting “based on downloads of a specific app or purchases within a specific app (including subscriptions) from the App Store, unless the targeting is done by that app’s developer.”

44. It is generally understood that Apple News has been a disappointment for Apple thus far.⁶⁰ However, Apple's substantial market power in adjacent markets means that it can cross-subsidise Apple News and disadvantage its competitors to ensure its success in the medium to long term.
45. Only a handful of global app developers have the scale to be competitive with a natively installed iOS app like Apple News. Every publisher has to put considerable effort into marketing in order to become known about, downloaded and then habitually engaged with by users. Often this involves promoting the app on the developer's website and paying Apple for promotion in the App Store. MailOnline uses millions of ad placements on its website each year to support the app. Many news organisations have given up trying to overcome the difficulties and have moved away from app development (to the detriment of users who prefer using apps to browsers on their handsets).⁶¹
46. In 2003, the Daily Mail introduced an online version of its newspaper, MailOnline, and in 2011 it overtook The New York Times as the world's most popular English-language newspaper website. The MailOnline app is free to use (with no premium tier). The costs of employing reporters, editors, photographers, video journalists, and running the app and website are paid for by selling advertising space alongside news articles. MailOnline decided not to join Apple News when it was rolled out in the UK, primarily because of its negative experience with Apple News in the US and Australia (where advertising revenue were underwhelming)⁶² and its desire to avoid cannibalisation of its UK app traffic.
47. As explained above, third-party publishers such as MailOnline will no longer be able to access IDFAs from most of their users' devices. But Apple will not be similarly hampered, as it will subject users to personalised advertising by default.
48. Apple's discrimination against third-party apps harms competition in four ways.

60 See e.g., Lucia Moses, "Apple News is sending publishers traffic, but not revenue", *Digiday*, 16 October 2016, available at <https://digiday.com/media/apple-news-sending-publishers-traffic-not-revenue/> (citing issues with monetizing traffic); William Turvill, "Platform profile for Apple News: the traffic is 'incredible' – but money is 'particularly bad'", *Press Gazette*, 20 October 2020, available at <https://www.pressgazette.co.uk/apple-news-pros-and-cons-for-publishers/> (noting that major publishers such as The Washington Post and The New York Times turned down the opportunity to become partners of Apple News+).

61 Nearly 90% of mobile internet time is spent in apps: <https://mindsea.com/app-stats/>.

62

49. **First**, the ATT solicitation will make it markedly more difficult for third-party apps to compete against Apple News. If publishers can no longer identify users for advertising purposes, publisher inventory will be worth substantially less. MailOnline has found that app inventory is worth [REDACTED] less without an IDFA. For many publishers, the hit to revenue may be so severe that they cannot survive. Many third-party apps may drop out of the market, leaving consumers with fewer choices, and leaving Apple with less competition for Apple News.
50. In July 2020, MailOnline’s Apple News traffic suddenly fell by [REDACTED] in the US and it was unable to get an explanation from Apple for this. Apple News therefore raises similar issues to the Google Search issues discussed in the digital advertising market study relating to sudden algorithmic changes that have a material effect on traffic to news and other content providers – both Google and Apple are gatekeepers with extraordinary power of life and death over competitors and customers. Some transparency and accountability is necessary.⁶³
51. The harm to competition is particularly acute in the market for online news compared with other services. Society benefits from a diverse cross-section of perspectives, but Apple’s opt-in rule threatens apps from ad-supported publications and potentially subscription-based applications that also rely on ad sales. The only news service that remains unharmed is Apple News. Apple News is essentially a news curation service. Apple licenses content from news outlets and features “Top Stories” at the top of the page, followed by traffic-driven “Trending Stories” beneath it. A news publisher that no longer can support its app could be forced to license its content to Apple, lest it lose out on an app-based distribution channel altogether.
52. The problem, though, is that Apple News creates a gatekeeper for news content, where Apple alone exercises editorial control over what users can see. The “Top Stories” at the top of an Apple News page are selected by Apple’s editors. If Apple News becomes a leading clearinghouse for app-based news content as competitors exit the market and license their content to Apple, there is a real risk that users will be deprived of a robust, diverse, politically balanced marketplace for news content. Apple is not well placed to choose the nation’s news. We cannot expect Apple to exercise its power to benefit anyone other than itself.
53. **Second**, for those apps that might get by in the short term, they eventually may have to adopt a subscription model to survive. Apps that cannot support themselves with targeted ads will have to charge users. That will put rival apps at a significant disadvantage compared to Apple News, which Apple can subsidise with revenue from other products. Further, even if the move to a subscription service is successful, the apps and their users

63 See e.g., CMA Final Report, paragraphs 8.13 and 8.16.

still will not emerge unharmed. News apps may fall within the reader rule, meaning that they may in theory disable Apple’s payment-processing service (“In-App Purchase”) to process subscriptions. However, many users will want to be able to sign up in the app rather than the website (to which the developer cannot direct them due to Apple’s anti-steering provisions). Where apps do not fall within the reader rule, In-App Purchases charges a 30% fee for subscriptions over the first year, followed by a 15% fee each year thereafter. That is a significant cost for publishers that will be passed to users. Thus, not only would users now be paying for once-free content, they also would be paying up to a 30% surcharge to Apple.

54. **Third**, if publishers can no longer access a device’s IDFA, then neither can their advertisers. The only way advertisers will be able to access targeting information when buying app inventory on an Apple device is by purchasing such inventory from Apple (i.e., the “Apple Ad Network”). That imposes a tie on advertisers: to access targeting information for app ads on an iOS device, advertisers must buy Apple’s app inventory and use Apple’s ad network. Advertisers must accede to the tie because there is no other comparable source of information when serving app ads on an Apple device.
55. Nor should we expect users to discipline Apple’s behaviour by buying a different device. When a user buys an iPhone or iPad, he or she cannot know – and thus cannot price in – all of the costs that Apple imposes in its app ecosystem. Moreover, switching devices now is cost prohibitive. iPhone and iPad users have made substantial investments in these devices and, in many cases, have taken out multiyear loans to fund their purchase.
56. **Fourth**, Apple gets valuable data from competing news services, whether they adopt a free-to-use or subscription model. It wedges itself in between app developers and their customers. It can engage in precisely the type of behaviour of which Amazon and Facebook are accused, i.e., using their competitors’ competitively sensitive information to decide whether to enter a market and, once it has entered, gain an unfair advantage.⁶⁴

64 See European Commission, Press release of 10 November 2020, “Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices”, available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2077; European Commission, Press release of 4 June 2021, “Antitrust: Commission opens investigation into possible anticompetitive conduct of Facebook”, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2848; Competition and Markets Authority, Press release of 4 June 2021, “CMA investigates Facebook’s use of ad data”, available at: <https://www.gov.uk/government/news/cma-investigates-facebook-s-use-of-ad-data>.