Konrad Kollnig, Reuben Binns, Nigel Shadbolt
Department of Computer Science
University of Oxford

4 February 2022

Response to the public consultation on mobile ecosystems by the Competition and Markets Authority

This document provides the response of researchers within the Department of Computer Science of the University of Oxford. We have been studying the data flows and power relations in the mobile ecosystem for many years, and would like to take the opportunity to share relevant research and perspectives with you.

Mobile ecosystems serve as an important part of our everyday lives, mediating social, political and market interactions. The ever increasing importance and ubiquity of mobile devices puts great power into the hands of those companies that make the key design decisions affecting mobile ecosystems. Decisions that might sometimes go against the interests of consumers. This is why we welcome the opportunity to respond to the ongoing investigation of the CMA into mobile ecosystems.

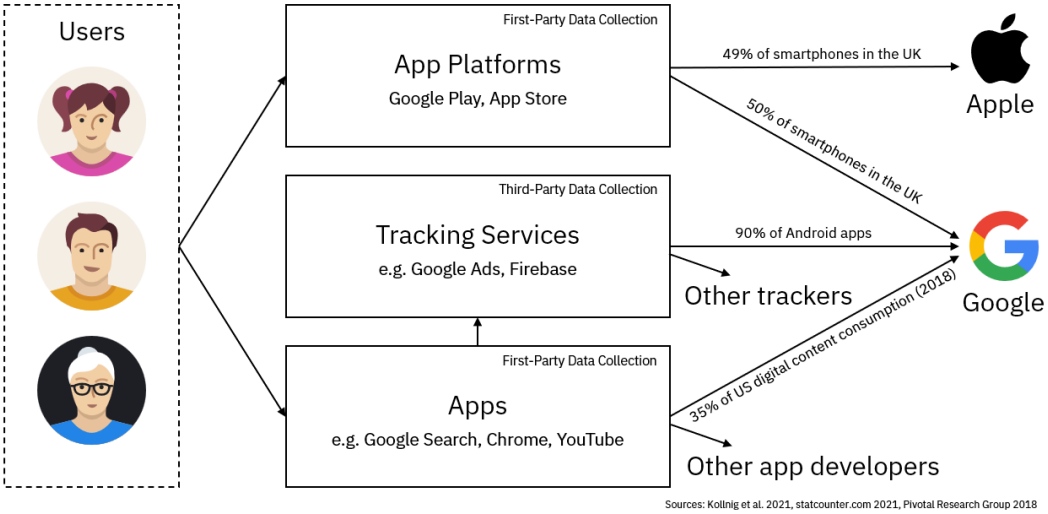


Figure 1. Illustration of data flows in the mobile ecosystem.

An illustration of the power distribution (emerging from access to personal data and integration of services) in the mobile ecosystem is shown in Figure 1 above. Apple and Google provide some of the core services in this ecosystem, and across different layers. This gives these companies a significant competitive advantage over competitors, by gaining important insights into the day-to-day practices of individuals and other businesses, particularly through pervasive, large-scale data collection ('tracking').

Summary of Recommendations

- Ensure that app developers are not (implicitly or explicitly) nudged into violating basic provisions of UK data protection law, particularly the need to seek consent before engaging in third-party tracking. This could include *standards for regulatory conformance* (e.g. clarifying the responsibility of those companies developing tracking technologies, and requiring them to provide simple and compliant implementation guidance to app developers), and should ultimately aim to build a mobile ecosystem that facilitates *compliance by default* (see Section 1.1.1).
- Empower researchers to conduct *app research*, by enabling ways in which researchers can more easily analyse encrypted iOS apps, download apps at scale, and analyse encrypted network traffic of apps on Android (see Sections 1.2.1–1.2.2).
- Enable researchers to analyse concerns around underlying technologies of the mobile ecosystem, including the use of data relating to individuals and other advertising companies in Apple's SKAdNetwork (see Section 1.4.3).
- Lower barriers to entry and innovation. Encourage the use of cross-platform technologies in app development (such as open web technologies), ensure that Windows and Linux users can develop apps for iOS (currently only macOS users), and lower the barrier to entry into the App Store (currently an annual 99 USD fee applies) (see Section 2.1).
- Ensure that gatekeepers do not self-preference, particularly with regards to ad attribution or in the definition of tracking in the Apple ecosystem, and the distribution of adblocking technologies on Android and in Google Chrome (see Sections 1.4.2–1.4.3 and 2.1).
- Scrutinise Google's current ban of in-app tracking blockers (see Section 2.1), including Disconnect.me, to give consumers more choice over how apps use their data and to tackle widespread infringements of data protection law (particularly the

need to seek user consent prior to tracking, as well as proportionality, data minimisation and purpose limitation) within apps.

- Consider requiring smartphone OS's and app store operators to enable third-party mobile app extension functionality to spur innovation in mobile apps and reduce harms within them, similar to the approach taken with extensions in desktop browsers and mobile Safari starting with iOS 15, while ensuring safety of consumers using such extensions through the existing app store review processes (see Section 2.2).
- Ensure that the review of apps on the app stores and the policies underlying this process are fair and transparent, for example through *regular mandatory disclosures* about this enforcement (including with regards to privacy and data protection). Such disclosures would be a minimally invasive but realistic intervention, and have been suggested by a variety of researchers from different backgrounds. See Section 3.1 for more details.
- Consider separating key functions within the governance of mobile ecosystems to reduce conflicts of interests, such as privacy management to avoid self-preferencing as regards data collection and protect consumers against excesses and monopolisation of such data collection, and promoting more research into this area (see Section 3.2).

1. Research on the Status Quo and Implications

In the past, our research group has conducted various pieces of research that have attempted to analyse both the market power of companies in the digital ecosystem, as well as the choice consumers have over their data and the services that they use. In particular, we conducted four relevant research studies in 2021 and published or are to publish these in relevant, well-regarded academic venues.

1.1. Study 1: Widespread absence of user choice over tracking

We studied a representative sample of 1,297 apps from the Google Play Store[1], and found that very few apps actually ask for consent prior to tracking consumers (less than 10%), while most apps (more than 70%) share data with a range of third-party companies before any user interaction. In our analysis, we did not determine what these tracking companies do with this collected data, or if it is, in fact, used to track users, because we as researchers have limited insights into the further data processing by tracking companies. Meanwhile, UK data protection law often requires consent to track users, as we also analyse in our paper. This paper recently won the annual Student Paper Award by the Future of Privacy Forum[2].

1.1.1. More technical guidance for app developers needed

An important reason for this lack of compliance is that existing guidance for app developers by trackers is often hard to find, poorly maintained and difficult to read, due to the inherent conflicts of interests of trackers in increasing data collection and getting integrated into apps while protecting user privacy.

Despite UK data protection law usually requiring consent to tracking, we found that Google and other companies do not make this point salient in their online implementation guidance for app developers and thereby make compliance for app developers harder than it might need be. To overcome the situation, trackers could provide more code samples of compliant implementation of their tracking technologies, thereby speaking the language of the developers and also taking on more responsibility for the use of their tools.

---

[1] Konrad Kollnig, Reuben Binns, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb and Nigel Shadbolt (2021). A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. *7th Symposium on Usable Privacy and Security (SOUPS 2021)*. https://www.usenix.org/conference/soups2021/presentation/kollnig

[2] Future of Privacy Forum. Privacy Papers for Policymakers. https://fpf.org/privacy-papers-for-policy-makers/

1.2. Study 2: Widespread violations of data protection principles on iOS and Android

We analysed a representative set of 24,000 apps from Android and iOS with regards to their privacy practices[3]. In both ecosystems, our study highlights widespread potential violations of US, EU and UK data protection and privacy law, including 1) the use of third-party tracking without user consent, 2) the lack of parental consent before sharing personal data with third-parties in children's apps, 3) the non-data-minimising configuration of tracking libraries, 4) the sending of personal data to countries without an adequate level of data protection, and 5) the continued absence of transparency around tracking, partly due to design decisions by Apple and Google (further discussed below).

1.2.1. Difficulty of app research due to gatekeeper design decisions

A key issue that emerged from our analysis across iOS and Android – besides the current failure to enforce existing data protection law in apps – is the lack of transparency around apps' data practices. Such transparency is essential in keeping and holding gatekeeper power to account, but the analysis thereof remains difficult in the mobile tracking ecosystem. This conflicts with the strict transparency requirements for the processing of personal data laid out in the UK-GDPR (Article 5). Design decisions by Apple and Google profoundly impede research efforts.

1.2.2. Challenges in conducting app research

In both ecosystems, the download of apps at scale is difficult for researchers, but essential in order to analyse mobile ecosystems at scale, which is in turn essential in understanding the ecosystem providers' impacts on privacy, security and the digital economy. In the EU, lawmakers are currently trying to give research more insights through Article 31 of the planned Digital Services Act, though current drafts have been criticised[4].

Beyond this, both ecosystems present further unique challenges as explained below. Apple applies encryption to every iOS app by default, even to free ones. Researchers must find ways around this encryption, which can drive them into legal grey areas because such

---

[3] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek and Nigel Shadbolt (2022). Are iPhones Really Better for Privacy? A Comparative Study of iOS and Android. *Proceedings of the Privacy Enhancing Technologies Symposium*. https://arxiv.org/abs/2109.13722

[4] Paddy Leerssen (2021). Platform research access in Article 31 of the Digital Services Act. https://verfassungsblog.de/power-dsa-dma-14/

encryption might fall under UK copyright law. As a result, there has been hardly any large-scale research into the privacy practices of iOS apps from 2013 until the 2021 paper by our research group. We have worked around some, but by far not all, the limitations in analysing iOS apps.

On Android, Google has been introducing various measures that are meant to increase user privacy and security, but have also made research significantly more difficult. The most notable of such measures are the **ban on installing self-signed certificates** (thereby preventing researchers from analysing apps' network traffic for app research without deep modifications of the system files of Android devices) and the roll-out introduction of the Google SafetyNet (which makes it impossible to run certain apps – including popular apps like Snapchat and Pokemon Go – on Android devices with modified system files). The roll-out of the SafetyNet and the ban on self-signed certificates in tandem makes app research like ours extremely difficult. While Google argued that the ban on self-signed certificates would serve device security, it seems that the company could easily implement choice architectures for average end-users to prevent them from accidentally installing such certificates (as is currently done on iOS where the installing of such certificates is not easy but possible), while still allowing researchers to disable such security features to conduct their work. Some internet outlets even declared the death of modifying the Android operating system (currently a central requirement for Android app research) in response to Google's rollout of the SafetyNet[5]. Additionally, many apps nowadays use code obfuscation, which further complicates app privacy research.

1.3. Study 3: Choice between trackers and afforded by the GDPR

We analysed 1 million apps from the UK Google Play Store from before the introduction of the GDPR, and 1 million from afterwards[6].

In this analysis, we found that the known market concentration in data collection from mobile devices has hardly seen any change (see Figure 2). For instance, 85% of apps from 2017 could send data to Alphabet, compared to 89% in 2020.

---

[5] JC Torres (2020). Google SafetyNet update might be the end for Android rooting, custom ROMs. https://www.slashgear.com/google-safetynet-update-might-be-the-end-for-android-rooting-custom-roms-30627121/

[6] Konrad Kollnig, Reuben Binns, Max Van Kleek, Ulrik Lyngs, Jun Zhao, Claudine Tinsman and Nigel Shadbolt (2021). Before and after GDPR: tracking in mobile apps. *Internet Policy Review, 10(4)*. https://policyreview.info/articles/analysis/and-after-gdpr-tracking-mobile-apps

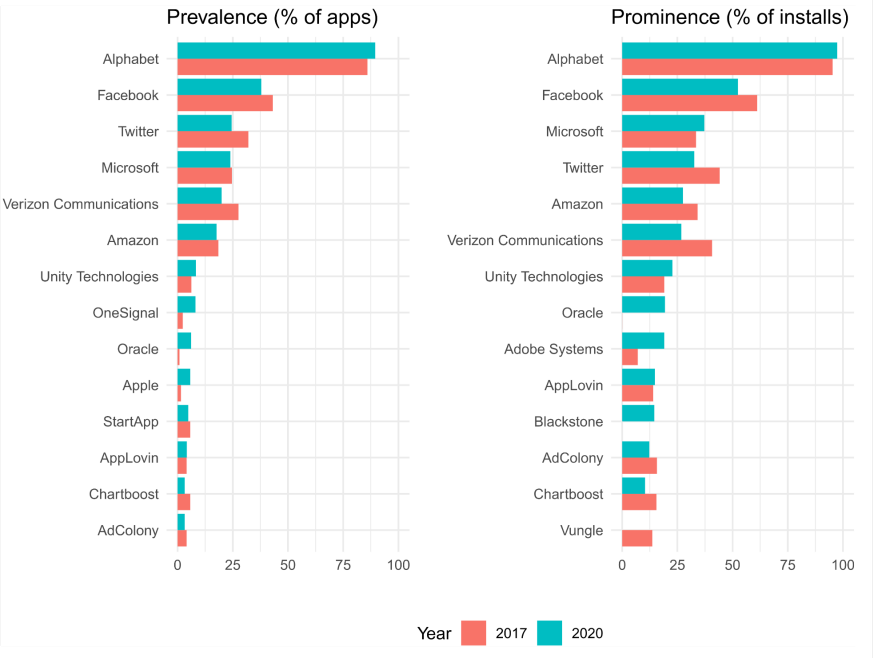


Figure 2. Prevalence and prominence tracking companies in the studied apps.

Our analysis also hints at a high level of concentration in the tracking market (see Figure 3), and some ongoing consolidation among tracking companies. We observed that only three of 53 observed M&A transactions in the tracking ecosystem between 2018 and 2020 were filed with EU or UK competition authorities.

Year	ISH-HHI	PROWISH-HHI	Gini
2017	0.112	0.071	0.491
2020	0.115	0.067	0.493

Figure 3. Various metrics for market concentration in third-party tracking show limited change and a level of concentration in the tracking market. For details, especially as regards the rather novel market concentration measures "ISH-HHI" and "PROWISH-HHI", consult our paper.

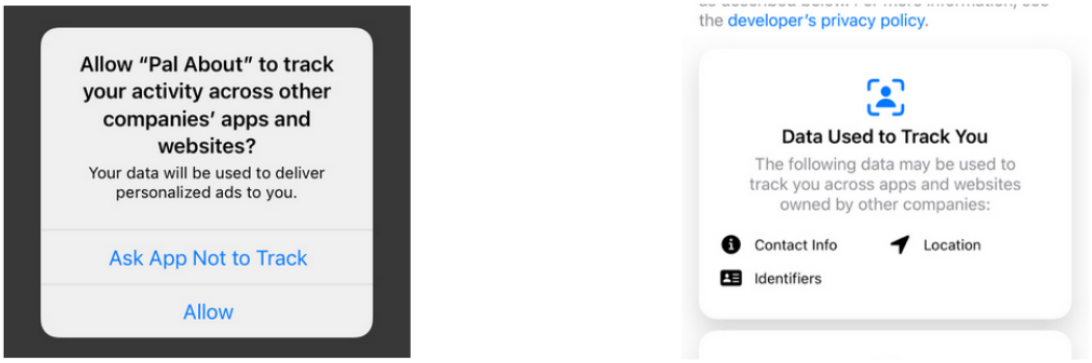
Our study suggests that current enforcement of data protection obligations does not yet achieve its intended ends, and that intervention by regulators is warranted, in particular

increased scrutiny of M&A transactions that concern data businesses[7] and stricter enforcement of existing data protection rules.

In our analysis, we did not analyse how tracking itself may have changed in response to the introduction of the GDPR – only the extent to which such tracking still takes place. Analysing the quality and invasiveness of tracking (rather than only its extent) is, however, difficult to accomplish, given that we as researchers do not usually have insights into what happens in the servers of tracking companies.

1.4. Study 4: Apple App Tracking Transparency

In ongoing (and not yet peer-reviewed) research[8], we are analysing the impact of Apple's new Privacy Nutrition Labels and App Tracking Transparency on app privacy, see Figure 4. Specifically, we looked at 1,759 iOS apps from the UK Apple App Store: one version from before iOS 14 and one that has been updated to comply with Apple's new rules.



(a) Apple Tracking Transparency (ATT). (b) Privacy Nutrition Label.

Figure 4. Overview of Apple's new privacy measures, introduced with iOS 14. Source: https://developer.apple.com/app-store/user-privacy-and-data-use/

We find that Apple's new policies, as promised, prevent the collection of the Identifier for Advertisers (IDFA), an identifier used to facilitate cross-app user tracking. However, the number of tracking libraries has – on average – roughly stayed the same in the studied apps.

[7] Reuben Binns, Elettra Bietti (2020). Dissolving privacy, one merger at a time: Competition, data and third party tracking. *Computer Law & Security Review 36*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269473

[8] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns and Nigel Shadbolt (2022). Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. *Submitted to the ACM Conference on Fairness, Accountability, and Transparency*

Counterintuitively, the average number of contacted companies and domains, and integrated opt-in permissions of iOS apps have seen a slight, but statistically significant, increase.

We also found that the Privacy Nutrition Labels can be inaccurate and mislead consumers about apps' actual privacy practices. For example, 80.2% of those apps, that declared not to collect any data in their Privacy Nutrition Labels, actually sent data to at least one known tracking company right at the app's first initiation, before any user interaction and thus without user consent. This observed phenomenon seems to be more widespread in apps that did not range among the top apps on the App Store. As before, we did not analyse the invasiveness of such tracking because we do not have insights into the further data processing of tracking companies, so some of this observed data sharing with tracking companies may not be problematic.

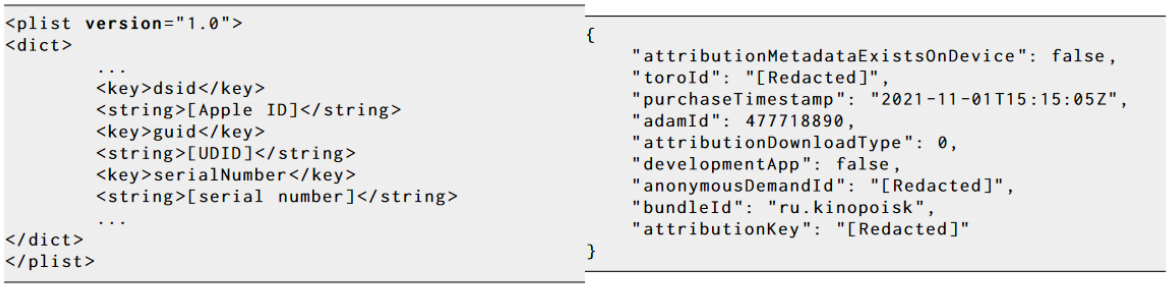
Overall, Apple's technical changes make tracking more difficult now, but also reinforce the market power of existing gatekeeper companies with access to large troves of first-party data. Smaller data brokers, who used to engage in some of the most egregious and invasive data practices, will now face much higher challenges in conducting their business – a positive development for end-users. We expect, however, that tracking companies will eventually work around these new policies, by using statistical methods ('fingerprinting') to identify users. Such fingerprinting would likely be easier to conduct for larger companies than smaller ones – deepening current imbalances in market power. A recent report by the FT confirms this, and also highlights that Apple might foresee ways for other large companies getting around the ATT rules – something that might be unexpected for consumers[9]. Despite the new rules, large companies, like Google/Alphabet and Facebook/Meta, are still able to track users across apps, because these companies have access to unique amounts of data about users. Out of similar concerns, the CMA is investigating Google's Privacy Sandbox, which would entail the removal of third-party cookies from its Google Chrome browser[10].

[9] Financial Times (2021). Apple reaches quiet truce over iPhone privacy changes.
https://www.ft.com/content/69396795-f6e1-4624-95d8-121e4e5d7839
[10] Competition and Markets Authority (2021).
Investigation into Google's 'Privacy Sandbox' browser changes.
https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes

1.4.1. ATT can be misleading and might lead to consolidation in tracking

We have concerns that Apple's new policies might disproportionately extend the advertising business of Apple, and might mislead consumers. Apple appears to orient its definition[11] of tracking around that of the W3C[12], when in fact, there are notable differences: Apple differentiates between first-party (which includes Apple's own data collection from the iOS operating system) and third-party data collection, and only considers third-party data collection harmful, when in fact, the effects on individual privacy can be similar. The W3C foresees no such distinction in its definition of tracking.

Since Apple apparently considers its own data collection from other developers' apps as being first-party, it does not consider that its own tracking practices fall under its tracking definition and continues to track users even when they opt-out of app tracking (see Figure 5). Some of Apple's own apps, including the App Store itself, have access to this information because they are not distributed via the App Store and hence might not need to comply with the rules governing apps on the App Store, including those that relate to the tracking of users.



(a) Request of Apple App Store to https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/renewVppReceipt?guid=[UDID].

(b) Request (shortended) of Apple's advertising framework to https://ca.iadsdk.apple.com/adserver/attribution/v2.

Figure 5. Sharing of unique user identifiers with Apple, even after having refused tracking.

A direct impact of Apple's definition might be that Apple's new policy will lead to more consolidation in the tracking market, so as to benefit from the privileges around first-party

[11] Apple (2021). User Privacy and Data Use. https://developer.apple.com/app-store/user-privacy-and-data-use/
[12] W3C Working Group (2019). Tracking Compliance and Scope. https://www.w3.org/TR/tracking-compliance/#tracking

tracking. Apple also includes certain kinds of *cohort tracking* and *credit scoring* from its definition of tracking, which might be unexpected and invasive for consumers[13].

1.4.2. Apple still has access to crucial device information and might self-preference

In our study, we observed that Apple still has access to a wide range of device identifiers that third-party app developers have no access to (see Figure 5). For example, we observed that Apple regularly collects the device's serial number (see Figure 5a), through which Apple can accurately tie the point-of-sale of its devices to activities on the device itself, and track the device lifecycle in great detail. This is information that competitors do not have access to, and might disproportionately privilege Apple's position in the smartphone ecosystem.

As a result of its competitive advantage, it has been reported that Apple has been able to triple its share in iOS advertising since the introduction of ATT[14].

As highlighted in the interim report of the consultation, Apple operates two different ad attribution mechanisms. We would like to point to analysis by Eric Seufert, who discusses in detail how Apple might use this to advantage its own advertising business[15]. Crucially, both attribution systems provide a different quality of insights, with Apple getting more valuable insights into ad attribution than competitors in iOS advertising.

1.4.3. Apple's potential collection about data about advertising competitors

There's a further concern that Apple might collect data about its competitors in mobile advertising, by effectively obliging these competitors to use the SKAdNetwork from now on. By making competitors use a standard library for advertising, Apple could potentially abuse its market position to collect data about the business and ad clicks of competitors, and use this data to make its own advertising system even more competitive. Apple does foresee explicitly in its privacy policy that it may collect data about users' interactions with its advertising technology, which would include data from the SKAdNetwork[16]. The company

[13] Apple (2021). User Privacy and Data Use.
https://developer.apple.com/app-store/user-privacy-and-data-use/
[14] Financial Times (2021). Apple's privacy changes create windfall for its own advertising business.
https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d
[15] Eric Seufert (2021). ATT advantages Apple's ad network. Here's how to fix that.
https://mobiledevmemo.com/att-advantages-apples-ad-network-heres-how-to-fix-that/
[16] Apple (2021). Apple Advertising & Privacy.
https://www.apple.com/legal/privacy/data/en/apple-advertising/

confirmed to us that this might be the case. Unfortunately, Apple has so far refused to provide detail on how their SKAdNetwork system processes personal data, following a series of GDPR requests submitted by us since August 2021. Apple's privacy policy provides no specific information on SKAdNetwork[17].

In our correspondence with Apple, the company has acknowledged the use of pseudonymous identifiers and Standard Contractual Clauses to send personal data relating to its advertising system to the USA as part of the SKAdNetwork. This would be incompatible with the ECJ's Schrems II ruling if no additional safeguards were implemented. The company has so far only provided very high-level information on such additional safeguards, and no information on whether personal data relating to its competitors in the advertising business are processed. This makes it impossible for us to assess this potential abuse of Apple's market power, and deepens our concerns.

Having filed a complaint with the ICO on 25 October 2021, the ICO responded on 14 January 2022 to say that there is more work for Apple to do in order to answer our questions around its use of personal data in SKAdNetwork (case reference IC-136750-H2X1).

2. Open Standards for a Competitive Mobile Ecosystem

2.1. Web Apps and Alternative Browser Engines

Currently, app developers must learn Java or Kotlin development for Android development, and Objective-C and Swift for iOS. iOS developers must additionally have access to Mac hardware (which is usually expensive) because Apple's Xcode programming environment is incompatible with Windows or Linux operating systems. Furthermore, both Apple and Google provide ecosystem-specific libraries and tools, such as the Google Play Services or the Apple App Insights. This certain lack of interoperability of development practices between mobile ecosystems might be holding back innovation. Moreover, the high annual fee of 99 USD to publish apps on the App Store might serve as a deterrent for small app developers to develop for iOS; Google only charges new app publishers a one-time payment of 25 USD.

[17] Apple (2021). Apple Advertising & Privacy. https://www.apple.com/legal/privacy/data/en/apple-advertising/

As the interim report points out, web apps are a promising way to develop apps for both platforms. They rely on open technologies that are already highly successful in underpinning the WWW and Internet as we know it, and can be developed from essentially any computer environment. At the moment, mobile web apps don't offer a competitive user experience to compete with native apps (i.e. those apps that are developed with the platform-specific programming languages and tools: Java or Kotlin on Android, and Objective-C and Swift on iOS). The experience in using these apps is generally not as 'smooth' as it would be with native apps, and many app users and developers don't like them. We don't see a technical reason why this must be the case. Famously, Mark Zuckerberg admitted in 2012 that "The biggest mistake we made as a company was betting too much on HTML5 as opposed to native. … It just wasn't ready."[18]; in response, Facebook developed React Native to enable app developers to develop cross-platform apps with a shared code base.

In the past, Mozilla Firefox tried to establish the model of interoperable apps based on open technologies with Firefox OS. This attempt failed, mostly because the system failed to reach a critical mass (due to existing natural monopolies). However, the example of Firefox OS shows that there's in principle no reason why web technologies could not underpin mobile ecosystems. In fact, it seems to be already done with React Native – at least to an extent.

WebExtensions (i.e. an open technology for browser extensions) are a good example of a similar ecosystem with an interoperable technology. The Google Chrome and Mozilla Firefox browser extension stores use the same format for such extensions (relying on web technologies), and thereby facilitate interoperability between the two different browser engines (i.e. Blink and Gecko). Publishing a browser extension is merely an act of uploading a ZIP archive of the browser extension (which itself is a collection of HTML and JavaScript files) to the Chrome or Firefox extension stores. The distribution of browser extensions also shows that these open technologies do not compromise on device security, because these extensions undergo a review process before publication.

We believe that, *ideally*, the publication of mobile apps should be as simple as developing and publishing browser extensions, by leveraging open and interoperable technologies, thereby leading to more innovation within the mobile ecosystem and overcoming existing hurdles to such innovation. This does not need to sacrifice privacy and security because

[18] Mashable (2012):"Zuckerberg's Biggest Mistake? 'Betting on HTML5'". https://mashable.com/archive/html5-biggest-mistake

apps would still be distributed through app stores and undergo the usual review processes. This might positively impact market power, privacy and security within these ecosystems, since web technologies are developed by multi-stakeholder committees and there exists a wide range of privacy-preserving technologies from the web that could more easily be applied in mobile ecosystems.

2.2. Extension stores for mobile apps to reduce online harms

Mobile ecosystems have emerged as locked-up ecosystems that isolate different apps for security and usability purposes. While on the web users are used to installing browser extensions, similar technology has not been allowed on mobile devices. There's no technical reason why this could not be the case. Apple has already introduced such with iOS 15, but limits them to its Safari browser[19]. Google has long been criticised for not extending the extension functionality from its desktop browser to its mobile browser (which would be technically straightforward, as shown by Apple who use a similar code base for their Safari browser and the fact that the Chrome desktop browser already integrates this functionality)[20].

On the web, the availability of browser extensions has led to a fruitful ecosystem of extensions that improve users' browser experience. These extensions help remove malware from websites, reduce unwanted distractions and dark patterns, reduce unwanted collection of personal data without consent and sometimes against UK data protection law (see Section 1.1), make it easier for disadvantaged users to participate by allowing them to make the web more accessible (e.g. through browser extensions that render any displayed text more readable for dyslexics), and generally reduce online harms (as acknowledged as an important problem, and currently targeted by the UK government[21]).

We have explored the use of extension technology to reduce online harms in a series of recent research in the context of mobile ecosystems[22]. Indeed, there are already solutions – such as Cydia Substrate (iOS), Magisk (Android) or the Xposed Framework (Android) – to

[19] MacRumors (2021). iOS 15 Safari Extensions Worth Checking Out. https://www.macrumors.com/guide/ios-15-safari-extensions/
[20] Google (2014). Chrome Developers: FAQ. https://developer.chrome.com/docs/multidevice/faq/
[21] UK Department for Digital, Culture, Media & Sport (2021). Draft Online Safety Bill. https://www.gov.uk/government/publications/draft-online-safety-bill
[22] Konrad Kollnig, Siddhartha Datta and Max Van Kleek (2021). I Want My App That Way: Reclaiming Sovereignty Over Personal Devices. *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. https://dl.acm.org/doi/10.1145/3411763.3451632 *and* Siddhartha Datta, Konrad Kollnig, Nigel Shadbolt (2022). Mind-proofing Your Phone: Navigating the Digital Minefield with GreaseTerminator. *ACM IUI 2022*. https://arxiv.org/abs/2112.10699.

allow users to improve certain aspects about the apps they use. Since these existing extension frameworks are not allowed on the official app stores, they do not undergo the usual review process – a problem that could potentially be fixed easily by supporting such technologies.

In the past, these app extension technologies have been targeted by the gatekeepers of mobile ecosystems – partly out of concern that the current approach is unregulated and must currently sidestep the usual app store review process. Most recently, the main developer behind Magisk was hired by Google and had to remove core functionality of Magisk as a result of obligations imposed by this new employer[23]. Moreover, Google currently bans any apps from its Play Store "that interfere with … other apps"[24]. This has in the past been the foundation of Google's ban of the popular Disconnect.Me service from the Play Store in 2014[25]. This service aimed to reduce unwanted data collection in other apps, which would be against Google's current policies. The result of the ban is that end-users have few protections against the known loss of privacy in digital devices, and potentially widespread infringements of UK data protection law in apps (such as the need to seek consent, and following the principles of data minimisation and purpose limitation).

Extension functionality could be extended from browsers to mobile apps so as to increase the competition around the best ideas and implementations on the app stores, and support the priorities of the UK government in reducing online harms.

In December 2021, we conducted a preliminary, non-representative survey with 100 UK participants. 85% indicated that such functionality would be useful to them, and 69% that they'd like to have a right to make such modifications.

[23] XDA (2021). Magisk is dropping support for hiding root access from apps. https://www.xda-developers.com/magisk-development-continues-without-magiskhide/
[24] Google (2021). Device and Network Abuse. https://support.google.com/googleplay/android-developer/answer/9888379
[25] TechCrunch (2015). Disconnect.Me Files Antitrust Case Against Google In Europe Over Banned Anti-Malware Android App. https://techcrunch.com/2015/06/02/disconnect-me-files-antitrust-case-against-google-in-europe-over-banned-anti-malware-android-app/

3. Transparency and Accountability around Gatekeeper Decisions

3.1. Mandatory app store transparency obligations

Greene and Shilton provided one of the few studies we found that systematically compared the influence and roles of app platforms on shaping user privacy in 2018[26]. They found that Apple and Google intervene in very different ways. While Apple imposes strict rules on its app ecosystem, which generally translates to user privacy benefits for most users, Google's ecosystem was mainly characterised by the absence of intervention. Google's approach has mixed implications for user privacy; 'The "wild west" of Android development means that privacy solutions abound for skilled hobbyists but that baseline privacy measures for the masses are lacking'. These authors concluded that, given the power of app platforms, there needs to be greater transparency around platform governance and enforcement of privacy rules.

Similarly, Van Hoboken and Ó Fathaigh argued in 2021 that Google and Apple increasingly act as important regulators of data protection and privacy, but with limited regulation, oversight, and accountability[27]. To increase transparency, these authors argued for mandatory disclosures about the privacy-related activities of smartphone platforms – **as a minimally invasive but realistic intervention**.

Mandatory privacy disclosures around the privacy actions of app platforms could be an important step to increase transparency and accountability within the app ecosystem easily, while posing very limited damage to the status quo. As highlighted by our analysis, the gatekeepers often fail to enforce simple requirements of the GDPR (as we observed in our own research discussed above in Section 1).

3.2 Structural separation within governance of mobile ecosystems

Another intervention to address problems in mobile ecosystems could be the introduction of structural separation within the governance of these ecosystems. One potential field for

[26] Daniel Greene, Katie Shilton (2017). Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media & Society, 20(4)*. https://journals.sagepub.com/doi/full/10.1177/1461444817702397

[27] Joris van Hoboken, R Ó Fathaigh (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review, 41*. https://www.sciencedirect.com/science/article/pii/S0267364921000303

intervention is privacy management, which is often in conflict with the interests of gatekeepers in data collection and the need to protect consumers from harmful data collection. However, it is beyond this response to discuss the different possible ways to leverage structural separation with the necessary detail that such would require.