PRIVACY
INTERNATIONAL

How Apps on Android Share Data with Facebook

(even if you don’t have a Facebook account)

December 2018

Privacy International is a UK-registered charity (1147471) that promotes the right to privacy at an international level. It is solely responsible for the research and investigation underpinning its reports.

Executive Summary

Previous research has shown how 42.55 percent of free apps on the Google Play store could share data with Facebook, making Facebook the second most prevalent third-party tracker after Google's parent company Alphabet.[1] In this report, Privacy International illustrates what this data sharing looks like in practice, particularly for people who do not have a Facebook account.

This question of whether Facebook gathers information about users who are not signed in or do not have an account was raised in the aftermath of the Cambridge Analytica scandal by lawmakers in hearings in the United States and in Europe.[2] Discussions, as well as previous fines by Data Protection Authorities about the tracking of non-users, however, often focus on the tracking that happens on websites.[3] Much less is known about the data that the company receives from apps. For these reasons, in this report we raise questions about transparency and use of app data that we consider timely and important.

Facebook routinely tracks users, non-users and logged-out users outside its platform through Facebook Business Tools. App developers share data with Facebook through the Facebook Software Development Kit (SDK), a set of software development tools that help developers build apps for a specific operating system. Using the free and open source software tool called "mitmproxy", an interactive HTTPS proxy, Privacy International has analyzed the data that 34 apps on Android, each with an install base from 10 to 500 million, transmit to Facebook through the Facebook SDK.

All apps were tested between August and December 2018, with the last re-test happening between 3 and 11 of December 2018. The full documentation, including the exact date each app was tested, can be found at https://privacyinternational.org/appdata.

Findings

- We found that at least **61 percent of apps we tested automatically transfer data to Facebook the moment a user opens the app**. This happens whether people have a Facebook account or not, or whether they are logged into Facebook or not.
- Typically, the data that is automatically transmitted first is events data that communicates to Facebook that the Facebook SDK has been initialized by transmitting data such as "App installed"

[1] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., 2018. Third Party Tracking in the Mobile Ecosystem. arXiv preprint arXiv:1804.03603.
[2] Brandom, J. (2018) 'Shadow profiles are the biggest flaw in Facebook's privacy defense', *The Verge*. Available at: https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (Accessed: 1 December 2018).
[3] For instance, in 2015 Facebook was fined by the Belgian Data Protection Authority ("DPA") for tracking the online activities of Belgian non-Facebook users through social plug ins (such as the like-button), cookies and invisible pixels on third-party web sites. See https://www.dataprotectionauthority.be/news/judgment-facebook-case. In 2017, Facebook was also fined by the French Data Protection Authority (CNIL) for different privacy violations, among them "unfair" tracking of users and non-users as they browse the internet, without offering users sufficient warning. https://www.ft.com/content/10f558c6-3a26-11e7-821a-6027b8a20f23

and "SDK Initialized". This data reveals the fact that a user is using a specific app, every single time that user opens an app.

- In our analysis, apps that automatically transmit data to Facebook share this data together with a unique identifier, the Google advertising ID (AAID). The primary purpose of advertising IDs, such as the Google advertising ID (or Apple's equivalent, the IDFA) is to allow advertisers to link data about user behavior from different apps and web browsing into a comprehensive profile. **If combined, data from different apps can paint a fine-grained and intimate picture of people's activities, interests, behaviors and routines, some of which can reveal special category data, including information about people's health or religion.** For example, an individual who has installed the following apps that we have tested, "Qibla Connect" (a Muslim prayer app), "Period Tracker Clue" (a period tracker), "Indeed" (a job search app), "My Talking Tom" (a children's' app), could be potentially profiled as likely female, likely Muslim, likely job seeker, likely parent.
- If combined, event data such as "App installed", "SDK Initialized" and "Deactivate app" from different apps also offer a detailed insight into the app usage behavior of hundreds of millions of people.
- We also found that **some apps routinely send Facebook data that is incredibly detailed and sometimes sensitive.** Again, this concerns data of people who are either logged out of Facebook or who do not have a Facebook account. A prime example is the travel search and price comparison app "KAYAK", which sends detailed information about people's flight searches to Facebook, including: departure city, departure airport, departure date, arrival city, arrival airport, arrival date, number of tickets (including number of children), class of tickets (economy, business or first class).
- Facebook's Cookies Policy describes two ways in which people who do not have a Facebook account can control Facebook's use of cookies to show them ads. **Privacy International has tested both opt-outs and found that they had no discernible impact on the data sharing that we have described in this report.**

Discussion

Facebook places the sole responsibility on app developers to ensure that they have the lawful right to collect, use and share people's data before providing Facebook with any data. However, **the default implementation of the Facebook SDK is designed to automatically transmit event data to Facebook**.

Since May 25, 2018 – the day that the EU General Data Protection Regulation (GDPR) entered into force - developers have been filing bug reports on Facebook's developer platform, raising concerns that the Facebook SDK automatically shares data before apps are able to ask users to agree or consent. On June

28, 2018, Facebook released a voluntary feature that should allow developers to delay collecting automatically logged events until after they acquire user consent. **The feature was launched 35 days after GDPR took effect and only works on the SDK version 4.34 and later.**

In response to this report, Facebook has stated in an email to Privacy International on 28 December 2018: "Prior to our introduction of the "delay" option, developers had the ability to disable transmission of automatic event logging data, **except for a signal that the SDK had been initialized.** Following the June change to our SDK, we also removed the signal that the SDK was initialized for developers that disabled automatic event logging." (emphasis added).

This "signal" is the data that we observe in our findings. We assume that prior to the release of this voluntary feature, **many apps that use Facebook SDK in the Android ecosystem were therefore not able to prevent or delay the SDK from automatically collecting and sharing that the SDK has been initialized**. Such data communicates to Facebook that a user uses a particular app, when they are using it and for how long.

Conclusion

Without any further transparency from Facebook, it is impossible to know for certain, how the data that we have described in this report is being used. This is particularity the case since Facebook has been less than transparent about the ways in which it uses data of non-Facebook users in the past.

Our findings also raise a number of legal questions. As this research was conducted in the UK we have focused on the relevant EU framework, namely EU data protection ("GDPR") and ePrivacy law (the ePrivacy Directive 2002/58/EC, as implemented by Member State laws)[4] as well as Competition Law. **An underlying theme is the responsibility of the various actors involved, including Facebook.**

[4] The European Commission published a proposal for an ePrivacy Regulation in January 2017, to update the Directive and align with GDPR. However, this legislation is still under negotiation.

Third Party Tracking

In October 2018, researchers at the University of Oxford[5] published a peer-reviewed study of 959,000 apps in the US and UK Google Play stores that revealed how data from smartphones is shared and harvested by 'third-party trackers', that is entities that collect data about users from first-party websites and / or apps.[6]

Most apps contain third-party trackers and many apps contain a large number of different trackers. Research by French research organization Exodus Privacy and Yale University's Privacy Lab, for instance, showed that more than three in four apps on Android contain at least one third-party "tracker" in 2017.[7]

The unprecedented scope of the Oxford research, however, uncovered the extent to which big tech companies like Google, Facebook, Microsoft and Twitter are the most prevalent trackers on free apps on Android. The researchers found that 90 percent of the apps analyzed could share data with Google's parent company Alphabet, while Facebook could receive data from 42.55 percent of apps.[8]

App developers integrate the technologies of 'third parties' in their mobile applications source code for a number of reasons: to track crash reports, measure user engagement (analytics) or to connect their app to social networks (for instance, by allowing users to share photos on Facebook from the app), and to generate revenue by monetizing user data and displaying behaviorally targeted ads.[9]

While tools developed by third parties can be useful for developers, those tools often also allow third parties to collect ("track") user data from the developer's 'first party' mobile apps for the third party's use.[10] In particular, third parties whose code is embedded in a large number of apps receive data about users that could be linked and combined into a detailed profile.

Mobile devices contain many different types of identifiers, such as information relating to the device, as well applications, tools or protocols that, when used, allow the identification of the individual to whom the information may relate.[11] Even in the absence of such identifiers, researchers have found that knowledge of any four apps installed on users' smartphones is enough to successfully track 95 percent

[5] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., 2018. Third Party Tracking in the Mobile Ecosystem. arXiv preprint arXiv:1804.03603.
[6] Ibid.
[7] https://exodus-privacy.eu.org
[8] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., 2018. Third Party Tracking in the Mobile Ecosystem. arXiv preprint arXiv:1804.03603.
[9] European Union Agency for Network and Information Security. (2017). *Privacy and data protection in mobile applications*. Available at: http://enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications (Accessed: 1 December 2018).
[10] Ibid.
[11] Information Commissioner's Office (2018). *What are identifiers and related factors?* Available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/ (Accessed: 1 December 2018).

of users.[12] Many third-parties also perform cross-device tracking[13], the practice of linking multiple devices, such as smartphones, television sets, smart TVs, and personal computers, to a single user. The more granular a user profile, the more intimate inferences can be derived about people's likely attributes, identities, habits and opinions.[14]

It is in this context that the prevalence of big tech companies in the tracking ecosystem raises concerns. Any company receives data from a considerable percentage of all apps, would be able to gain a particularly deep insight into the everyday behavior and interests of mobile phone users.

Why third-party tracking on apps raises unique privacy challenges

Privacy International has recently asked regulators to investigate a number of data broker and advertising technology companies ("AdTech") that constitute a complex back-end system that is used to direct advertising to individuals and specific target audiences.[15] At a generalized level these companies track individuals around the web and across different apps and help dictate what advertising content they see.[16]

Despite having trackers throughout the web, many third parties are not household names. Most people have never heard of them, do not know that they process their data and profile them, whether this data is accurate, for what purposes they are using it, or with whom it is being shared or what the consequences are. Quantcast, a company that Privacy International has investigated as part of these complaints, for instance, claims that it can collect real-time insights on audiences on over 100 million mobile and web destinations[17]. A member of Privacy International's staff has described the picture Quantcast was able to obtain about her life, from the data gathered through a single cookie placed on one of her browsers alone.[18] In our complaints we argued that this exploitation of the personal data of millions of people in the European Union and further afield constitutes an infringement of data protection law.

Third-party tracking in both mobile apps and on the web raises important human rights concerns, in particular concerning the right to privacy and data protection. Third party tracking on apps usually happens in the background, which means that many users are unaware of the fact that third parties are

[12] Achara, J.P., Acs, G. and Castelluccia, C., 2015, October. On the unicity of smartphone applications. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society* (pp. 27-36). ACM.

[13] Brookman, J., Rouge, P., Alva, A. and Yeung, C., 2017. Cross-device tracking: Measurement and disclosures. *Proceedings on Privacy Enhancing Technologies*, 2017(2), pp.133-148.

[14] Privacy International (2018). *A Snapshot of Corporate Profiling*. Available at: https://privacyinternational.org/feature/1721/snapshot-corporate-profiling (Accessed: 1 December 2018).

[15] Privacy International (2018). *Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad*. Available at: https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad (Accessed: 1 December 2018).

[16] Privacy International (2018). *Submission to the Information Commissioner – Request for an Assessment Notice / Complaint of Adtech Data Brokers.* Available at: https://privacyinternational.org/sites/default/files/2018-11/08.11.2018%20Final%20Complaint%20AdTech%20Criteo%2C%20Quantcast%20and%20Tapad.pdf (Accessed: 1 December 2018).

[17] https://www.quantcast.com/data-hub/

[18] Privacy International (2018). *I asked an online tracking company for all of my data and here's what I found.* Available at: https://privacyinternational.org/feature/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found (Accessed: 1 December 2018).

tracking them. What makes tracking on mobile apps uniquely challenging is that it is much easier to block or reduce tracking on both mobile and desktop web browsers than it is in apps.

The rationale of this report: why we are focusing on third-party tracking by Facebook

The purpose of this report is to illustrate one way in which mobile apps on the Android operating system share data with large tech companies. For this report, we focused on Android (instead of other operating systems or devices), however, third party tracking is prevalent on other platforms as well. We were specifically interested in the kinds of data that apps share with Facebook about users that do not have a Facebook account (or that are logged-out of the platform), as well as when and how this data is being transmitted. While others have looked at the prevalence of tracking more broadly[19], we have focused on Facebook because their access to data as a third party comes in an unusual and unexpected way for consumers.

Facebook routinely tracks users, non-users and logged-out users outside its platform through Facebook Business Tools. For instance, any website that has integrated a Facebook like button or tracking pixel automatically sends data to Facebook.

As outlined in Facebook's UK data policy, this information includes "information about your device, websites you visit, purchases you make, the ads you see and how you use their services – whether or not you have a Facebook account or are logged into Facebook."[20]

App developers share data with Facebook through the Facebook Software Development Kit (SDK), a set of software development tools that can be used to develop applications (Apps) for a specific operating system. Facebook's SDK for Android allows app developers to integrate their apps with Facebook's platform and contains a number of core components: Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links. For example: Using Facebook's SDK, allows for support of "Login with Facebook" based authentication, which allow users to login using a phone number of email address with their Facebook password. Facebook's SDK also offers Analytics (data, trends, and aggregated audience insights about the people interacting with the app), as well as Ads and reading and writing to Facebook's Graph API.

This question of whether Facebook gathers information about users who are not signed in or do not have an account was raised in the aftermath of the Cambridge Analytica scandal by lawmakers in hearings in

[19] Information Society Project Yale Law School Privacy Lab. Available at: https://privacylab.yale.edu/press.html (Accessed: 1 December 2018).
[20] Facebook UK Data Policy. Available at: https://en-gb.facebook.com/policy.php (Accessed: 1 December 2018).

the United States and in Europe.[21] Discussions about the tracking of non-users, however, often focus on the tracking that happens on websites.[22] Much less is known about the data that the company receives from apps.

Facebook has also not always been very transparent about the ways in which is uses data is collects. For instance, in September 2018, researchers at Northeastern University and Princeton found that Facebook allows advertisers to target people based on contact information they handed over for security purposes and contact information that was collected from other people's contact books, [23] or what the journalist Kashmir Hill calls "shadow contact information".[24]

For these reasons, in this report we raise questions about transparency and use of app data that we consider timely and important.

Selection Criteria and Methodology

A research group at the Computer Science department of the University of Oxford, the authors of the aforementioned study on "Third Party Tracking in the Mobile Ecosystem", provided Privacy International with a list of the top 1,000 apps (in terms of install base) that likely transmit data to Facebook.

These 1,000 apps constitute the most installed apps of the 42.55 percent of ~1 million Android apps that the researchers identified as likely transmitting data to Facebook. The authors identified apps that likely transmit data to Facebook (and other trackers) by identifying references to hosts in apps' Android Package Kit (APK) - an Android file format that contains all resources needed by an app to run on a device.

[21] Brandom, J. (2018) 'Shadow profiles are the biggest flaw in Facebook's privacy defense', *The Verge*. Available at: https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (Accessed: 1 December 2018).

[22] For instance, in 2015 Facebook was fined by the Belgian Data Protection Authority ("DPA") for tracking the online activities of Belgian non-Facebook users through social plug ins (such as the like-button), cookies and invisible pixels on third-party web sites. See https://www.dataprotectionauthority.be/news/judgment-facebook-case. The Belgian DPA's action was based on KU Leuven University's research revealing that Facebook's privacy policies breach European law. This comprehensive study, drafted at the request of the Belgian Privacy Commission, outlines the different data collection techniques, such as cookies, pixels, social plug-ins and other similar technologies used by Facebook to build up user and non-user profiles. See https://www.law.kuleuven.be/citip/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation. The Belgian DPA's decision was challenged by Facebook on grounds of jurisdiction, however in February 2018 the Belgian Court of First Instance once again ruled that Facebook violated privacy laws (see legal analysis below) by deploying technology such as cookies and social plug-ins to track internet users across the web. The court ordered Facebook to stop tracking Belgians' web browsing habits and destroy any illegally obtained data. https://www.dataprotectionauthority.be/news/victory-privacy-commission-facebook-proceeding. In 2017, Facebook was also fined by the French Data Protection Authority (CNIL) for different privacy violations, among them "unfair" tracking of users and non-users as they browse the internet, without offering users sufficient warning. https://www.ft.com/content/10f558c6-3a26-11e7-821a-6027b8a20f23

[23] Venkatadri, G., Lucherini, E., Sapiezynski, P. and Mislove, A., 2019. Investigating sources of PII used in Facebook's targeted advertising. *Proceedings on Privacy Enhancing Technologies*, 1, p.18.

[24] Hill, K. (2018) 'Facebook Is Giving Advertisers Access to Your Shadow Contact Information'. *Gizmodo*, 26 September, Available at: https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051 (Accessed: 1 December 2018).

As described in more detail in the paper's data collection and methodology section: "Upon download, each APK was unpacked and decoded using APKTool[25] to obtain the app's assets, in particular its icon, bytecode (in the DEX format) and metadata (in XML format). Finally, permission requests were parsed from the XML and hosts were found in the bytecode using a simple regex."[26]

In a next step, references to hosts were mapped with lists of known trackers: "Host names in the tracker lists were shortened to 2-level domains using the python library tldextract4 (e.g. for 'subdomain.example.com', the domain name 'example' and top-level domain suffix '.com' were kept and any subdomains were omitted). Tracker hosts were then matched to hosts identified in app bytecode with a regular expres- sion which excluded matches that was followed by a dot or an alpha- betic character (matching 'google.com' to 'google.com/somepath' but not 'google.com.domain' or 'google.coming')." [27]

An inherent limitation of this methodology, as explained at length in the paper, is that it is impossible to know if the presence of code relating to or referencing to known tracker hosts also means that these hosts are ever called. In other words: the presence of code is indicative of tis use, but doesn't actually mean it is ever called by the application. To confirm if apps actually share data, and to further understand what kind of data is shared when, we selected 34 apps for further manual analysis from the original list of 1,000 apps (see Appendix 1). We choose apps whose purpose suggests potentially sensitive data (health, faith etc.) and apps that are either well-known, or have a large install base.

Analysis

Privacy International's testing components consisted of the following components:

- A laptop running a Virtual Machine (using Oracle's VirtualBox) with mitmproxy in "transparent" mode (meaning that the connection is being intercepted without the knowledge of the client). Along with the necessary tools to create a functional network access point. The Virtual Machine is running Debian 10 (Buster/Unstable) due to the requirements of mitmproxy using python 3.6.4 or later.
- A Nexus 5 Android Phone, Running Android 8.1 (Oreo) – we used Lineage OS, built from the Android Open Source Project (AOSP), in order to run later versions of Android on the device.
- A device (laptop) to run the Android Development Bridge (ADB) in order to install the mitmproxy certificate into the Systems Trust Store (as opposed to the Users Trust Store) due to security

[25] Taylor, V.F. and Martinovic, I., 2017, April. To update or not to update: Insights from a two-year study of android app evolution. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 45-57). ACM.
[26] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., 2018. Third Party Tracking in the Mobile Ecosystem. arXiv preprint arXiv:1804.03603.
[27] Ibid.

constraints introduced in Android 7[28], and to screen record actives undertaken in apps using the "screenrecord" functionality of ADB.

All data being transmitted between Facebook and apps is encrypted in transit using Transport Layer Security (TLS, formally SSL). Our analysis consisted of capturing and decrypting data in transit between our own device and Facebook's servers (so called "man-in-the-middle") using the free and open source software tool called "mitmproxy", an interactive HTTPS proxy. Mitmproxy works by decrypting and encrypting packets on the fly by masquerading as a remote secure endpoint (in this case Facebook). In order to make this work, we added mitmproxy's public key to our device as a trusted authority. The data exists on our local network at time of decryption.

A new Google Account was setup for the sole purpose of this research and a full phone "nandroid" backup was taken so the device could quickly be returned to a known state, particularly considering that when some apps are installed and run, they continue to run in the background potentially polluting the results.

All session data that traversed mitmproxy ("flows") where recorded and stored, so they could be analyzed further.

- All session data that traversed mitmproxy ("flows") where recorded and stored, so they could be analyzed further, and shared later should the need arise.
- The screen and interactions where recorded as video using the Androids Developer Bridge (ADB) all activity that takes place on the screen of the Android device is recorded
- The outputs of each tests where then stored in Privacy Internationals internal knowledge management system with appropriate comments on the activity observed.

Once this was completed and appropriate setting within the phone where selected (pertaining to Wi-Fi, certificate trust, security such as PIN and screen lockout and developer tools such as showing touches) a full phone "nandroid" backup was taken so the device could quickly be returned to a known state, particularly considering that when some apps are installed and run, they continue to run in the background potentially polluting the results.

- After each wipe the following steps where undertaken
- Connect to a non-intercepting Wi-Fi
- Download the Application from the Google Play Store
- Connect to mitmproxy VM (via Wi-Fi), and create a new flow

[28] Android 7 Nougat and certificate authorities. Available at: https://blog.jeroenhd.nl/article/android-7-nougat-and-certificate-authorities (Accessed: 1 December 2018).

- Start Screen Recording using ADB
- Open the app, and do various activities for up to 320 seconds (if the app requires sign up to use, Google account created at the start of the process)
- Save screen recording off the phone and stop the flow in mitmproxy
- Reboot to recovery and restore the nandroid backup, ready to restart the process
- Reboot the device

Findings

Observation 1 – at least 61 percent of all apps tested automatically transfer data to Facebook the moment a user opens the app

Of the Android apps tested, a majority automatically transmit data to Facebook. This happens whether people have a Facebook account or not, or whether they are logged into Facebook or not.

Typically, the first data that is automatically transmitted is events data that communicates to Facebook that the Facebook SDK has been initialized by transmitting events data such as "App installed" and "SDK Initialized."

The events data that is shared contains information about the version of the SDK used, the user's unique Google advertising ID (AAID), as well as the app's unique name in the Google Play Store. It also includes extraneous data such as the app version, the device name (e.g Nexus 5), the version of Android, the screen resolution and information, such as the input Language of the device (en_GB) and the device timezone [Europe/London].

After the app has been initialized, we observed that apps share other events data such as "App closed" or "App Opened".

Our findings indicate that 23 out of 34 apps tested communicated the following information to Facebook about users who do not have a Facebook account (or that are logged out of the platform):

- The fact that a user is using a specific app
- Every single time that user opens and closes an app
- Information about the nature of the device the user owns, and the user's suspected location based on language and time zone settings

Observation 2 – The data that Facebook receives is linked to the Google ad ID, a unique identifier

In our analysis, apps that automatically transmit data to Facebook share this data together with a unique identifier, the Google advertising ID (AAID). As we have mentioned above, knowledge of any four apps installed on users' smartphones is enough to successfully track 95% of users.[29] However, since the data that is received is already linked to a unique identifier, it would be especially easy to combine data about a user's behavior from different apps into a profile.

The Google advertising ID (AAID) is a unique, user-specific ID for advertising, provided by Google Play services, that is automatically assigned to each Android user.[30] The primary purpose of advertising IDs, such as the Google advertising ID (or Apple's equivalent, the IDFA), is to allow advertisers to link data about user behavior from different apps and web browsing into a comprehensive profile. In Privacy International's complaints against the ad tech companies Quantcast, Criteo and Tapad, for instance, we describe how advertising companies collect user identifiers for the purpose of linking different browsers and mobile apps (sometimes called "ID syncing").[31] Criteo, for instance, specifically mentions in its privacy policy that it is collecting mobile advertising IDs (such as the Google AAID) for the purpose of ID syncing.[32]

If combined, data from different apps can paint a fine-grained and intimate picture of people's activities, interests, behaviors and routines, some of which can reveal special category data, including information about people's health or religion.

For example, an individual who has installed the following apps that we have tested, "Qibla Connect" (a Muslim prayer app), "Period Tracker Clue" (a period tracker), "Indeed" (a job search app), "My Talking Tom" (a children's' app), could be potentially profiled as:

- Likely female
- Likely Muslim
- Likely job seeker
- Likely parent

Since August 2014, Google requires that all services related to advertising targeting and tracking on Android use AAID in lieu of other identifiers, such as persistent device IDs.[33] Google allow users to reset

[29] Achara, J.P., Acs, G. and Castelluccia, C., 2015, October. On the unicity of smartphone applications. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society* (pp. 27-36). ACM.

[30] Play Console Help – Advertising ID. Available at: https://support.google.com/googleplay/android-developer/answer/6048248?hl=en (Accessed: 1 December 2018).

[31] Privacy International (2018). *Submission to the Information Commissioner – Request for an Assessment Notice / Complaint of Adtech Data Brokers.* Available at: https://privacyinternational.org/sites/default/files/2018-11/08.11.2018%20Final%20Complaint%20AdTech%20Criteo%2C%20Quantcast%20and%20Tapad.pdf (Accessed: 1 December 2018).

[32] Ibid.

[33] Android Developers – Advertising ID. Available at: http://www.androiddocs.com/google/play-services/id.html (Accessed: 1 December 2018).

(and thereby change) their Advertising ID in their phones' Google settings[34]. However, we found that unless a user actively changes their Advertising ID, it stays persistent. For instance, we found that the Advertising ID doesn't change when a device is reset to its factory settings if the user logs into the Android device using the same Google account.

In an e-mail to Privacy International on 29 December 2018 Google stated:

> "This is inaccurate. We would expect that a factory reset of the device would have the effect of generating a new Advertising ID. We tested a couple of devices we had on hand, and confirmed that the Advertising ID was changed upon factory reset, regardless of whether the user signed in with the same Google account or not. If you are seeing other behavior, it would be useful to know the precise specifications of the device and version of Android. In general, the Advertising ID does remain the same until it is reset by the user — which the user can do at any time for any reason."

Privacy International was unable to independently verify Google's tests on different devices. If accurate, it could mean that the behavior we observed is specific to our testing environment. We have shared details about our testing environment with Google.

Observation 3 – Some apps routinely transmit additional data to Facebook, some of which is highly granular

We also found that some apps routinely send Facebook data that is incredibly detailed and sometimes sensitive. Again, this concerns data of people who are either logged out of Facebook or who do not have a Facebook account.

A prime example is the travel search and price comparison app "KAYAK", which sends detailed information about people's search behavior on the app to Facebook. For example, when searching for flights between London and Tokyo, the app shares the following information, including:

- Timestamp of the search
- Name of the app
- Google advertising ID
- Departure city

[34] Ibid.

- Departure airport
- Departure date
- Arrival city
- Arrival airport
- Arrival date
- Number of tickets, including number of children
- Class of tickets (economy, business or first class)

A number of other apps, such as Duolingo or Instant Heartrate, share how the app is used, which menus the user has visited, and other interaction information. This is in addition to the data transmitted, as described in Observation 2.

Observation 4 – It is difficult to avoid being tracked by Facebook by apps on Android

Facebook's Cookies Policy[35] describes two ways in which people who do not have a Facebook account can control Facebook's use of cookies to show them ads:

> "You can opt out of seeing online interest-based ads from Facebook and other participating companies through […] the European Interactive Digital Advertising Alliance in Europe or through your mobile device settings. Please note that ad blockers and tools that restrict our cookie use may interfere with these controls."[36]

Privacy International has tested both opt-outs and found that they had no discernible impact on the data sharing that we have described in this report.

Android device settings don't prevent data sharing with Facebook

Devices running Android 6.0 and up afford users control over some of the data that each app is permitted to collect.[37] These settings, however, do no control the automatic transmission of the data we have described in this report.

Google also allow users to "Opt out of Ads Personalization"[38] on Android, which will apply across both Google ads services (ex: Search ads) and the 2+ million websites and apps that partner with Google to

[35] Facebook defines cookies broadly, including "identifiers associated with your device, and other software, are used for similar purposes".
[36] Facebook Cookie Policy (Date of Last Revision: 4 April 2018). Available at: https://www.facebook.com/policy/cookies/printable, (Accessed: 1 December 2018).
[37] This includes things like location and access to contacts, but not things like a devices' battery level and, crucially, access to the devices' current ad ID.
[38] Depending on your smartphone model, this can be found in the Google Ad settings in the main Settings menu or hidden away somewhere else.

show ads. Opting out of ads personalization, however, does not necessarily mean that users opt out of third-party tracking. We have tested the setting for the Skyscanner app, the KAYAK app and Shazam and found that the apps still share the same amount of data with Facebook, regardless of whether this setting is turned on or off.

In an e-mail to Privacy International on 29 December 2018 Google stated:

> “This is inaccurate. If a user disables “ads personalization” in the device Advertising ID settings, no app or ad vendor may use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising. This is true for Google apps, like Google Search, Maps and YouTube, but it is also true for all other apps installed on the device. This requirement is established via the Play Developer terms.
>
> Separately, Google users can disable ads personalization via a control in the Google Account controls. This will stop Google advertising services from creating user profiles for advertising purposes or for targeting users with personalized advertising. Opting out of ads personalization via the Google Account control will automatically apply on any device where the user signs in to his or her Google account.”

Privacy International believes that this statement above does not contradict our findings. Apps may not be allowed to use the advertising identifier for creating user profiles for “advertising **purposes** or for targeting users with personalized advertising” (emphasis added), but that does not prevent them from tracking users, that is collecting the data in the first place, or for using this data for other purposes.

The EEDA offers no tool that prevents the tracking we have described in this report

The European Interactive Digital Advertising Alliance (EEDA) is a self-regulatory initiative that offers “control solutions” through its website http://youronlinechoices.eu. This tool is designed to block tracking via cookies on mobile and desktop web browsers and as such, is unable to block tracking on apps that is done through technologies like the Facebook SDK instead of cookies.

Other alternatives to prevent tracking via the Facebook SDK on Android

End-users with appropriate expertise could manually block graph.facebook.com on the network level (via their router) or even on the device (using a firewall such as AFWall+ or NetGuard). Both these solutions require a level of expertise and understanding as to the implications of making such changes, and also may not fully stop data being sent to Facebook.

Observation 5 – Facebook only complied with our data subject access after several follow-ups

Data protection law in the EU (the EU General Data Protection Regulation "GDPR") provides that individuals have a number of rights in relation to their personal data, including the right to information about how their data is processed, the right to access their data, together with the rights to rectify, erase, restrict, port and object to the processing of their data.

- On October 29, 2018, a member of staff submitted an access request via the online form that Facebook provides for non-users of its platform[39], requesting access to all personal data relating to the Google advertising ID that was used in conducting this research. The rationale behind this access request was to gain further understanding about the ways in which Facebook uses the data it receives from apps and for how long it is being stored.
- Facebook auto responded on October 29, 2018, asking the user to confirm that they don't have a Facebook account, asking whether the users has had a previous account associated with their email address, as well as a detailed explanation of the information the user is requesting.
- On October 29, 2018 the member of staff confirmed that their email address is not (and has never been) associated with a Facebook and requested all personal data that is associated with their Google Advertising ID.
- On October 30, 2018 Facebook responded: "we couldn't find a Facebook account associated with **the email address** you're using to contact us. If you have a Facebook account associated with a different email address, please submit a new report." (emphasis added)
- On November 29, 2018 the member of staff sent a reminder.
- On December 6, 2018, the staff member sent another reminder.
- On December 20, 2018 Facebook responded that there were "unable to locate any personal data processed about you by Facebook, other than in connection with this request."

We will follow up on this request in 2019.

Discussion

Why do so many apps share data with Facebook the second they are initialized?

The default implementation of the Facebook SDK is designed to automatically transmit event data to Facebook. This is clearly stated in Facebook's Analytics Quickstart Guide for Android, which states:

[39] https://www.facebook.com/help/contact/2032834846972583

> "When you use the Facebook SDK, some events in your app are automatically logged and collected for Facebook Analytics unless you disable automatic event logging." [40]

Facebook places the sole responsibility on app developers to ensure that they have "the lawful right to collect, use and share [people's] data before providing [Facebook] with any data". [41] The company's Business Tool Terms[42] further require developers to notify individuals when they are using Facebook technology (including pixels, SDKs, and APIs) that enables Facebook to collect and process data about those individuals and obtain their prior informed consent for the developers' use of such tools:

> "If you use our pixels or SDKs, you further represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Customer Data collection […] In jurisdictions that require informed consent for storing and accessing cookies or other information on an end user's device (such as but not limited to the European Union), **you must ensure, in a verifiable manner, that an end user provides the necessary consent before you use Facebook Business Tools to enable us to store and access cookies or other information on the end user's device.**" (emphasis added)

While Facebook acknowledges that using the SDK requires user informed consent and also demands that developers to obtain this consent, developers have been filing bug reports on Facebook's developer platform, **raising concerns that the Facebook SDK automatically shares data before they are able to ask users to agree or consent to the processing**.

For instance, on May 29, four days after the GDPR entered into effect in the EU, a developer posted:

> "Hi all. We analized network activity of Facebook SDK for Unity and found that on application start it sends some requests to graph.facebook.com. It seems to be violation of GDPR: we can not send anything about a user until he allows us to do that. Could you please fix that or strongly confirm that these requests don't violate GDPR" [43]

A Facebook employee responded that the developer "should not have to worry about this specific request." [44]

On June 8, 2018, the same developer opened another bug report, repeating their concerns, this time about their iOS App using Unity SDK 7.12.2:

[40] Facebook Analytics Quickstart Guide for Android. Available at: https://developers.facebook.com/docs/analytics/quickstart-list/android/ (Accessed: 1 December 2018).

[41] Facebook Privacy Policy (Date of last revision: 19 April 2018). Available at: https://www.facebook.com/about/privacy/update/printable (Accessed: 1 December 2018).

[42] Facebook Business Tool Terms (Effective date: 25 May 2018). Available at: https://www.facebook.com/legal/terms/businesstools (Accessed: 1 December 2018).

[43] https://developers.facebook.com/support/bugs/290527161487564/?disable_redirect=0 (Accessed: 1 December 2018).

[44] Ibid.

> "We can't send user IDFA and other personal info until it is permitted by user, but we can't prevent it because FB SDK sends it on app start. This request needs to be moved to SDK inititalization which is called after a user accepts license agreement."[45]

In response to the thread, on June 18, 2018, another developer confirmed that IDFA (Apple's ad ID) is also being reported to Facebook prior to login on Android.[46]

A third bug report was filed on July 24, 2018, by a developer who notes:

> "When integrating the Facebook login SDK into android we realized, that when initializing the SDK a request is sent to the Graph API server, which includes an App-ID and an Advertising ID. Unfortunately this isn't compliant with the GDPR Guidelines, because the users haven't yet agreed to the privacy terms when starting the app. This is also the case , when the automatic events are deactivated. At the moment we have to avoid the problem with a workaround, which however leads to crashes. From our point of view the Facebook SDK should be initialized at a later stage or the request should only be sent after the user agreed to the terms. Please help us as soon as possible, as otherwise we are not allowed or able to use the Facebook SDK to login into our Android app." [47]

On July 25, 2018 an employee of Facebook responded to the third report that the issue has been resolved through a new SDK feature. The voluntary feature was released on June 28, 2018 and should allow developers to delay collecting automatically logged events until they acquire user consent. Developers need to upgrade to the latest Facebook SDK version, either iOS SDK v.4.34 or Android SDK v.4.34 to use this feature and the events that are included are: app install and app launches.[48]

The feature was launched 35 days after GDPR took effect. We assume that prior to the release of this voluntary feature, many apps that use Facebook SDK in the Android ecosystem were not able to delay collecting automatically logged data before they acquired user consent.

In an email to Privacy International Facebook has stated on 29 December 2018 (see Appendix):

> *"An app developer can get a user's consent to collect and process their data (including sending it to Facebook via the SDK). They can also choose to disable automatic event logging. Earlier this year, we also introduced a new option that allows developers to delay collection of app analytics information. […] in June of this year we introduced another option for businesses that want to use our auto-event logging feature if they choose not to use a pre-install mechanism for obtaining*

[45] https://developers.facebook.com/support/bugs/2049684891939638/?disable_redirect=0 (Accessed: 1 December 2018).
[46] Ibid.
[47] https://developers.facebook.com/support/bugs/1630827217043614/?disable_redirect=0 (Accessed: 1 December 2018).
[48] Facebook Ads News – New Privacy Compliance and Protections for GDPR. Available at: https://developers.facebook.com/ads/blog/post/2018/05/10/compliance-protections-gdpr/ (Accessed: 1 December 2018).

> *the prior consent contractually required. The legal and contractual obligation is on the developer (data controller) to get consent as required from their users before sharing personal data with Facebook via the SDK, and we wanted to provide another tool in the toolbox to help developers fulfill their legal and contractual obligations, while also providing a good experience for their users.*
>
> *[…] Prior to our introduction of the "delay" option, developers had the ability to disable transmission of automatic event logging data, **except for a signal that the SDK had been initialized.** Following the June change to our SDK, we also removed the signal that the SDK was initialized for developers that disabled automatic event logging.*
>
> *In June we also introduced another option for businesses that want to use our auto-event logging feature in compliance with our Business Tools Terms. Today, an app developer can either choose to use a pre-installed mechanism for obtaining an end-user's prior informed consent (as they could in the past), or use the SDK delay feature."* (emphasis added).

This "signal" is the data that we observe in our findings. We assume that prior to the release of this voluntary feature, **many apps that use Facebook SDK in the Android ecosystem were therefore not able to prevent or delay the SDK from automatically collecting and sharing that the SDK has been initialized**. Such data communicates to Facebook that a user uses a particular app, when they are using it and for how long.

Despite these options that Facebook describes, 61 percent of the apps that we have tested automatically transmit data to Facebook the moment the app is launched. There are different possible explanations for the behavior we observed. Since the SDK's default configuration is designed to automatically transmit data, it could be the case that apps simply use the default. We also observed that some apps run older versions of the SDK that wouldn't allow then to use the voluntary feature as it was designed. Skyscanner, for instance was running version 4.33.0 of the Facebook SDK on December 2nd, 2018 and Spotify was running version 4.31.0 on December 3rd. The feature only works on the Facebook Android SDK v.4.34.0 or newer [49]

It is also notable that developers continue to file bug reports, complaining that their apps automatically transmit data via the SDK, even after Facebook has released the aforementioned voluntary feature. For instance, developers have filed bug reports about the SDK transmitting data even when disabling auto

[49] Ibid.

events in August[50], October[51] and November[52] of 2018. This raises the question whether the voluntary feature that was released on June 28, 2018 works in practice.

In an email to Privacy International Facebook has stated on 29 December 2018:

> *"The voluntary feature that we released on June 28, 2018 for the Android SDK worked as we described at the time of launch. Following the launch, we received feedback from developers and made changes to (1) expand the information that we did not collect during the delay period, and (2) make the delay functionality available in our Unity SDK, which is separate from the Android SDK."*

How does Facebook use the data it receives about non-users of its platform?

In response to questions by the U.S. Senate Committee on the Judiciary in June 2018, Facebook responded to questions about its tracking of non-users and declared that:

> "Facebook does not create profiles for people who do not hold Facebook accounts. […] We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. **We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see**. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook."[53] (emphasis added)

[50] https://developers.facebook.com/support/bugs/1630827217043614/?disable_redirect=0 (Accessed: 1 December 2018).
[51] Ibid.
[52] https://developers.facebook.com/support/bugs/2049684891939638/?disable_redirect=0 (Accessed: 1 December 2018).
[53] Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing before the Committee on the Judiciary, Senate, 115th Cong. (2018), (Written answers for the record by Facebook, Inc). Available at: https://www.judiciary.senate.gov/imo/media/doc/Zuckerberg%20Responses%20to%20Judiciary%20Committee%20QFRs.pdf.

This statement seems to apply directly to the data that we have observed in this report. It suggests that Facebook does not create "profiles" for non-Facebook users and that data collected about them through app logs are not used to show targeted ads or to personalize the content they see.

Showing targeted ads and personalizing content, however, are just two possible uses for such data. Facebook's business tools terms describe a number of additional uses of "event data", that is the data that we have described throughout this report:[54]

> i. **Contact information for matching**
>
> 1. You instruct us to process the Contact Information solely to match the Contact Information against Facebook's or Instagram's user IDs ("**Matched User IDs**"), as well as to combine those user IDs with corresponding Event Data. We will delete Contact Information following the match process.
>
> ii. **Event Data for measurement and analytics services**
>
> 1. You instruct us to process Event Data (a) to prepare reports on your behalf on the impact of your advertising campaigns and other online content ("**Campaign Reports**") and (b) to generate analytics and insights about your customers and their use of your apps, websites, products and services ("**Analytics**").
> 2. We grant to you a non-exclusive and non-transferable licence to use the Campaign Reports and Analytics for your internal business purposes only and solely on an aggregated and anonymous basis for measurement purposes. You will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party, unless otherwise agreed to in writing by us. We will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party without your permission, unless (i) they have been combined with Campaigns Reports and Analytics from numerous other third parties and (ii) your identifying information is removed from the combined Campaign Reports and Analytics.
>
> iii. **Event Data to create targetable audiences**
>
> 1. We may process the Event Data to create audiences (including website Custom Audiences, mobile app Custom Audiences and Offline Custom Audiences) that are grouped together by common Event Data, which you may use to target ad campaigns. In our sole discretion, we may also allow you to share these audiences with other advertisers.
>
> iv. **Event Data to deliver commercial and transactional messages**
>
> 1. We may use the Matched User IDs and associated Event Data to help you to reach people with transactional and other commercial messages on Messenger and other Facebook Company Products.
>
> v. **Event Data to personalise features and content and to improve and secure the Facebook products**
>
> 1. We use Event Data to personalise the features and content (including ads and recommendations) that we show people on and off our Facebook Company Products. In connection with ad targeting and delivery optimisation, we will: (i) use your Event Data for delivery optimisation only after aggregating such Event Data with other data collected from other advertisers or otherwise collected on Facebook Products; and (ii) not allow other advertisers or third parties to target advertising solely on the basis of your Event Data.
> 2. We may also use Event Data to promote safety and security on and off the Facebook Company Products, for research and development purposes and to maintain the integrity of and to improve the Facebook Company Products.

The uses described in Facebook's business tools terms depend on the kind of Facebook Company Product apps and websites chose to use. The SDK contains a number of core components: Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links and apps can choose to use these features selectively. Since the data transmission we have observed in this report, however happens automatically and this independently from the component that an app uses, it is unclear which uses apply. For instance,

[54] Facebook Business Tool Terms (Effective date: 25 May 2018). Available at: https://www.facebook.com/legal/terms/businesstools (Accessed: 1 December 2018).

it is unclear whether the data could be used "for research and development purposes and to maintain the integrity of and to improve the Facebook Company Products."

It is also unclear whether Facebook's commitment to the US Senate to not create "profiles for non-Facebook users" refers to profiling in the sense of creating a Facebook profile, ready for them to use should they decide to join, or whether it refers to profiling in the sense of EU data protection ("GDPR"). The latter would include practices like identity matching, another purpose that is described in Facebook's business tools terms.

Without any further transparency from Facebook, it is impossible to know for certain, how the data that we have described in this report is being used. This is particularity the case since Facebook has been less than transparent about the ways in which it uses data of non-Facebook users in the past.

Sealed US Court Documents that were seized and published by the UK Parliament on December 5, 2018 raise new questions about the ways in which Facebook uses the data of people who do not have a Facebook account.[55] The documents confirm earlier reports by the Wall Street Journal[56] that Facebook used a Facebook-owned app called Onavo to gain insight into the usage of other mobile apps by Onavo customers, such as about how many people had downloaded which apps and how often they used them. The published internal documents, however, provide evidence that suggests that this knowledge helped Facebook to decide which companies to acquire, and which to treat as a threat.

Facebook acquired Onavo in 2013 and the released documents originate from a lawsuit that was originally filed in 2015. The Onavo app was still in use until Apple removed it from the App store in August 2018. It is unclear whether Facebook used the data it obtained from Onavo to gain insight into people's app usage until August 2018. For the purpose of this report, however, it should be noted that the data transmission we have documented in this report would allow the company to gain very similar knowledge.

Facebook has also been less than transparent when it comes to the ways in which the data of non-Facebook users are used to improve features. The above mentioned US Court Documents confirmed in Exhibit 172 that Facebook used data it obtained through the Android 'call log permission', a permission that gave Facebook continuous access to people's SMS and call log history, and that many users were unaware of for years,[57] to improve features like PYMK (People You May Know) suggestions and newsfeed

[55] UK Parliament (2018), 'Note by Damian Collins MP, Chair of the DCMS Committee – Summary of key issues from the Six4Three files', Available at: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf (Accessed: 1 December 2018).

[56] Seetharaman, D. (2018) 'Facebook Removes Data-Security App From Apple Store'. *The Wall Street Journal*, 22 August, Available at: https://www.wsj.com/articles/facebook-to-remove-data-security-app-from-apple-store-1534975340 (Accessed: 1 December 2018).

[57] Gallagher, S., 'Facebook scraped call, text message data for years from Android phones [Updated].' *arsTechnica*, 24 March, Available at: https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/ (Accessed: 1 December 2018).

ranking.[58] Facebook used this data for features it provided to people who have a Facebook account, but the fact that people's contacts, phone logs and SMS logs are used for such wide purposes, raises questions about how the company treats the data about non-users that is inevitably part of this processing.

In an email to Privacy International Facebook has stated on 29 December 2018:

> *"We do want to make sure that we are transparent about the data we collect and use. Our Data Policy (which is our primary privacy notice) and Cookies Policy describes the ways in which we collect data and the uses for which we may process that data, including how we use data from partners. For example, Facebook provides users the ability to authenticate with third-party apps in an easier way through Facebook Login product. Developers can receive analytics that allow them to understand what the audience of their app enjoys and improve their apps over time. Developers may also use Facebook services to monetise their apps through Facebook Audience Network. Subject to that Facebook user's prior consent, Facebook may also use this data to provide that user with more personalised ads."*

While Facebook should be more transparent, apps should also be transparent and upfront the purposes for which the data they share is being used.

Is this lawful?

The findings raise a number of legal questions. As this research was conducted in the UK we have focused on the relevant EU framework, namely EU data protection ("GDPR") and ePrivacy law (the ePrivacy Directive 2002/58/EC, as implemented by Member State laws)[59] as well as Competition Law. An underlying theme is the responsibility of the various actors involved, including Facebook.

Data Protection

Obtaining data on and from a device, including the transmission of data linked to a unique identifier from an app to Facebook via the Facebook SDK, constitutes the processing of personal data. Data relating to the use of specific apps, including usage logs, from which an individual is directly or indirectly identifiable is also personal data. Processing of personal data must comply with the legal obligations in the GDPR, including the data protection principles set out in Article 5, the requirement to have a lawful basis for

[58] UK Parliament (2018), 'Note by Damian Collins MP, Chair of the DCMS Committee – Summary of key issues from the Six4Three files', Available at: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf (Accessed: 1 December 2018).

[59] The European Commission published a proposal for an ePrivacy Regulation in January 2017, to update the Directive and align with GDPR. However, this legislation is still under negotiation.

processing personal data under Article 6, as well as the obligation to implement data protection by design and by default under Article 25.

Responsibility

More generally, however, there are open questions about the distribution of responsibility and legal obligation between app developers and third parties, including those that provide technologies and receive data in return, as is the case with the Facebook SDK. The GDPR assigns different obligations depending on the role a party has in data processing: the data controller and the data processor. The data controller has to comply with the central obligations in GDPR. In many cases this will be the App providers, however in some cases, there might be more than one controller in relation to the processing of personal data on an app and depending on who it is shared with. The European Union Agency for Network and Information Security (ENISA), for instance, has stated that "[t]his will be the case when an app integrates other data-driven functionality into the app, such as a third-party service provider for authentication of users or advertisement networks for monetization. In addition, the operating system may be gathering data when apps are used."[60]

Developers who click "accept" or are using any of the Facebook Business Tools, which include APIs and SDKs, the Facebook pixel, social plugins such as the Like and Share buttons, Facebook Login and Account Kit, agree to Facebook's terms, which require developers who use pixels or the SDKs "provided robust and sufficiently prominent notice to users regarding the Customer Data collection, sharing and usage." Controllers in the EU and in Switzerland furthermore need to agree to the following:

"To the extent the Customer Data contain personal data which you process subject to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR") , the parties acknowledge and agree that for purposes of providing matching, measurement, and analytics services described in Paragraphs 2.a.i and 2.a.ii above, that you are the data controller in respect of such personal data, and you have instructed Facebook Ireland Limited to process such personal data on your behalf as your data processor pursuant to these terms and Facebook's Data Processing Terms, which are incorporated herein by reference. "Personal data", "data controller" and "data processor" in this paragraph have the meanings set out in the Data Processing Terms."

However, Facebook cannot simply shirk responsibility for the data transmitted to it via Facebook's SDK by imposing contractual terms on others such as App developers or providers.[61]

[60] European Union Agency for Network and Information Security. (2017). *Privacy and data protection in mobile applications*. Available at: http://enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications (Accessed: 1 December 2018).

[61] Facebook Business Tool Terms (Effective date: 25 May 2018). Available at: https://www.facebook.com/legal/terms/businesstools (Accessed: 1 December 2018).

This issue of joint responsibility has been considered by the Belgian Court, in a decision upholding a decision of the Belgian DPA that found Facebook jointly responsible with website providers for its online tracking, namely through the Facebook pixel.[62] The same assignation of responsibility could be applied in the App context through the use of the Facebook SDK. Where Facebook maintains an element of control over the data received through the design of and default settings of the Facebook SDK and, importantly, controls the purposes and means for which the data transmitted to Facebook from the App via the Facebook SDK is processed, then Facebook could be considered a data controller.

The Belgian Court flagged the need for Facebook to provide "complete transparency about its data processing" and found that "…both the Facebook account holders and unregistered Facebook users need to consent to the placement of all cookies and not only some of them. As indicated above, this is a problem, as **Facebook makes it insufficiently clear that it is systematically collecting personal data when they visit a third-party website that contains Facebook social plug-ins, even if they have no Facebook account or are no longer logged in on Facebook**." (emphasis added)

The Belgian Court went on to criticize the opt out options offered by Facebook for users as well as highlighting the issues faced by non-users, "When non-users visit a website of a third party that includes an (invisible) Facebook pixel that allows for tracking of browsing behaviour, without indicating that they wish to make use of the Facebook service, no information mechanism (such as a banner) is displayed. The distributed Facebook information channels (Cookie Banner, Cookie Policy, Data Policy) contain equally little information about cookies, pixels and social plug-ins of third parties."

One of the arguments made by Facebook in this case was that "it is fulfilling its obligation as a provider of Facebook pixels for third-party websites by concluding binding agreements with them as well as requiring (via the general conditions) that this third party must *"provide definite and sufficiently visible notice of obtaining the necessary consent of the users",* including, among other things *"a clear and prominent notice on each web page that makes use of Facebook tools which is linked to a clear explanation"* and regularly reminding them of their obligations [and] it obliges third-party web application developers to provided "suitable notice" of the fact that *"third parties, including Facebook, may make use of cookies, web beacons and other storage technologies to collect or receive information from your websites, apps and elsewhere on the internet".*

However, the Court agreed with the Belgian Privacy Commission and upheld that, **as Facebook determines both the objective and means of processing, it remains the party responsible for processing personal data via pixels and is thus jointly responsible with the owners of the third-party websites for meeting the legal obligations.** The court found that the declarations

[62] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Facebook_judgment_16022018.pdf

which Facebook imposes on third parties in any case contain insufficient information about the fact that Facebook uses its cookies and pixels systematically to follow the browsing behavior of visitors to these websites, *even* if they have no Facebook account or are not logged in, so that this can also not be used to derive any valid consent. Facebook consequently does not show that it does or does not provide sufficient information to non-Facebook users via the owners of the third-party websites and obtains their valid consent." *(emphasis added).*

The Belgian Court found that in relation to non-account holders Facebook did not obtain any legally valid consent in the sense of Article 5.a. Privacy Act and Article 129 ECA for the disputed data processing. These articles implemented in Belgium the obligations under 1995 Data Protection Directive (which preceded GDPR) and the 2002 ePrivacy Directive provisions (covered below).

The question as to who may be regarded as a controller of the processing of personal data has also been considered by the European Court of Justice. The Court has been clear that the concept of 'controller' may concern several actors taking part in that processing, with each being subject to the applicable data protection provisions.[63] The purpose of the broad definition being to ensure effective and complete protection of the persons concerned.

Furthermore, the Court has stated that the 1995/56 Directive (the EU data protection law prior to GDPR) does not support a finding that the determination of the purpose and means of processing must be carried out by the use of written guidelines or instructions from the controller. However, a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller of the processing of personal data.[64]

As set out in this report Facebook has a principle role in controlling the design, implementation and operation of the SDK which enables the data from the Apps to be transmitted to Facebook together with a role in determining the purposing and means of processing of the data that Facebook receive. Therefore, considering the above jurisprudence and the aim to ensure effective and complete protection of the individuals whose data is processed, regardless of the contractual terms imposed via Facebook, Facebook should be considered a joint data controller together with the providers of the Apps.

[63] See judgment of 5 June 2018,*Wirtschaftsakademie Schleswig-Holstein* C-210/16 paragraphs 28 and 29; and judgment of 10 July 2018, *Jeohvan todistajat* C-25/17, paragraphs 65 and 66

[64] See judgment of 10 July 2018, *Jeohvan todistajat* C-25/17, paragraphs 67 and 68

Legal Basis

Analogies can be drawn with these cases both in terms of the Facebook's responsibility for processing, but also in terms of questions as to the legal basis (under Article 6 of GDPR) for Facebook processing personal data received from the Apps. It appears from Facebook's policy quoted above that Facebook seeks to place the responsibility with the Apps for only transmitting data that has been obtained lawfully. From an overview of the App Privacy Polices, where the Apps policies' mention third party tracking and Facebook specifically, they appear to be relying on a mix of legal basis under GDPR for third party tracking, namely consent, necessary for the performance of a contract and their legitimate interest. Facebook also rely on a combination of these bases for the majority of their data processing,[65] although as noted above, it appears that in the case of the data received via the Facebook SDK they are relying on consent obtained via the App.

Each of these bases are problematic for a number of reasons.

Consent

Article 4(11) of GDPR defines 'consent' for the purposes of the GDPR as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* From our analysis of the Apps it does not appear that such consent is being obtained. In the majority of the cases no specific information is provided to users about data being provided to Facebook via the SDK nor is any specific consent sought. If anything, there is just a general bundled request to agree to an App's terms of services and privacy policy. Furthermore, it appears that under the default implementation of the SDK, personal data is transmitted to Facebook before an individual has had the opportunity to be provided with further information or to consent to such data sharing. Even where a link to the Privacy Policy is provided in the Play Store it is questionable whether this satisfies the threshold of consent and clicking on download would be sufficient to constitute an unambiguous indication of the data subject's wishes. Nor does there appear to be any ability to withdraw consent to Facebook's processing and continue using the App. Thus, even if some form of consent is obtained, it seems tokenistic at best and not to meet the threshold of a freely given, specific, informed and unambiguous indication of the data subject's wishes. To the extent that the processing is covered by ePrivacy legislation, consent would be the only valid legal basis and thus raises questions where this is not obtained.

[65] Facebook Privacy legal basis. Available at:https://www.facebook.com/about/privacy/legal_bases (Accessed: 1 December 2018).

Contract

To the extent that the legal basis relied on is that the processing, i.e. the transmission of the data to Facebook via the SDK, is necessary for the performance of a contract to which the data subject is party, this is also problematic. For this condition to be met it must be demonstrated that the processing is necessary, i.e. the same aim could not be achieved in a manner that interferes less with an individuals' rights and that the sharing of this data is really needed in order to provide the App's services.[66] Facebook's provision of the voluntary feature, that delays the transmission of data, suggests that automatic transmission on the initiation of an App is not necessary. Making such automatic transmission a default feature, therefore, is a questionable practice. It is not at all clear that such processing by Facebook of the data is necessary for the performance of the contract between the App provider and the user.

Legitimate Interest

A controller that relies on legitimate interest as a basis for processing personal data must meet a three-part test. The data controller must identify a legitimate interest (purpose); show that the processing is necessary to achieve it (necessity); and balance it against the individual's rights and freedoms (balancing).[67] From the available information, it is not clear that any such assessments have been carried out. Recital (47) of GDPR makes clear that what is legitimate should turn at least in part on whether a legitimate interest is served due to the relationship between the controller and subject. However, via the Facebook SDK used by the apps, Facebook is receiving data on users with no Facebook account (thus no relationship with them) with no demonstrable regard and consideration for their rights and interests. This raises question as to whether Facebook could rely on legitimate interest as a basis for the processing.

Special Category Personal data

Certain types of data receive higher protections under GDPR, including data about individual's health, sex life, ethnicity/race, biometric data, genetic data, trade union membership and religion. In certain cases, the fact that an individual has downloaded and uses an app may reveal special category personal data about an individual and this may then be data transmitted via the Facebook SDK (and other third parties). For instance, the fact that someone has installed a prayer time app reveals a user's religious believes and the fact that a user uses a specific medical apps may indicate that they are affected by a particular medical condition. Such processing is prohibited unless a legal basis for processing such data under Article 9 of GDPR as supplemented by national laws is met. In the context of commercial Apps and

[66] See for example, the ICO's explanation of when is processing "necessary" https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ and South Lanarkshire Council v. The Scottish Information Commissioner [2013] UKSC 55 , paragraph 27.

[67] As explained in the ICO Guidance https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ and the Article 29 Working Party Opinion 08/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

platforms it is likely that the only available legal basis would be explicit consent. Given the issues raised above with consent, if the apps transmit special category personal data to Facebook via the SDK there are therefore questions as to whether a legal basis is met.

Principles

Lawfulness and legal basis are not the only data protection issues raised. That the majority of the apps tested automatically transmit "App Events" to Facebook, including a unique identifier, as well as logs containing usage data related to specific apps, is at odds with key principles of data protection namely, transparency, fairness, data minimization and purpose limitation.

From the analysis of the Apps together with an overview of the privacy policies, there is an evident lack of transparency – it is not made clear to people that Facebook is processing their data, how and for what purposes. This is intrinsically linked to fairness, which includes the requirement to consider the reasonable expectations of individuals, the effect that the processing may have on them and their ability to exercise their rights in relation to that information. It is questionable that it would be in the reasonable expectations of any users of the Apps tested that their data be shared with Facebook the second they use the App. The expectation of non-Facebook users is likely even lower. From the limited and high level information provided by Facebook about the use of such data (for example in the Business Terms quoted above) makes it difficult to assess the effect the processing may have on individuals, but what is clear as discussed elsewhere in this report is that it makes it difficult (i) to avoid having one's data processed by Facebook even as a non-user and (ii) to exercise one's data rights.

The default implementation of the Facebook SDK also appears to maximize as opposed to minimize the amount of data that is collected and then shared with Facebook. As indicated earlier in this report, apps may use the Facebook SDK for a number of reasons, however, the availability of a feature that delays transmitting data the second the app is opened, appears to indicate that such sharing is not necessary by default. Thus, this processing appears to be in contradiction of the principles of data minimization.

Data Protection by Design and Default

Furthermore, the Facebook SDK is problematic in view of the new GDPR obligation of data protection by design and by default. Article 25(2) of the GDPR requires that controllers "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." As set out in this report, the design of the Facebook SDK together with the default Facebook SDK implementation does exactly the opposite, namely automatically (by default) transferring personal data to Facebook for unspecified purposes.

ePrivacy

The findings of the report raise not just data protection questions but specific ePrivacy questions. Among other things, the ePrivacy Directive as implemented by Member State legislation governs confidentiality of communications which includes storing information in or gaining access to information stored in the terminal equipment[68] of a subscriber or user. This is the so called "Cookie law", which requires that subject to certain exceptions,[69] users must be provided with clear and comprehensive information and provide their consent. Since GDPR took effect, the definition and conditions of consent under ePrivacy is now equivalent to GDPR, meaning that consent has to be informed, explicit, unambiguous and specific.

These provisions apply to a range of actors, "Article 5(3) dealing with the use of cookies and similar techniques, which applies to anyone storing information or gaining access to information already stored, in the terminal equipment (i.e. computer, smart phone) of a subscriber or user."[70]

Given that via the Facebook SDK, Facebook is accessing information stored on smart phones (on which the Apps are installed), it is thus also relevant to consider the ePrivacy framework to apply to SDKs in the App environment.

On June 7, 2012, the Article 29 Data Protection Working Party published an opinion on the cookie consent exception. The opinion states that social networks need consent to collect data through social plug-ins about non-members of their network:

"…many social networks propose "social plug-in modules" that website owners can integrate in their platform, to provide some services than can be considered as "explicitly requested" by their members. However, these modules can also be used to track individuals, both members and non-members, with third party cookies for additional purposes such as behavioral advertising, analytics or market research, for example.

With such purposes, these cookies cannot be deemed to be "strictly necessary" to provide a functionality explicitly requested by the user. Therefore, these tracking cookies cannot be exempted under CRITERION B. Without consent, it seems unlikely that there is any legal basis for social networks to collect data through social plug-ins about non-members of their network. **By default, social plug-ins should thus not set a third party cookie in pages displayed to non-members**." [71] (emphasis added)

[68] "Terminal equipment" is defined in another EU Commission Directive 2008/63/EC on competition in the markets in telecommunications terminal equipment as: "equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network."

[69] "technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user." – Article 5(3) of the Directive.

[70] EU Commission background document on the consultation which lead to the draft e-privacy regulation

[71] Article 29 Data Protection Working Party Opinion 04/2012 on Cookie Consent Exemption, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf (Accessed: 1 December 2018).

The opinion doesn't mention mobile apps, but two separate arguments support the interpretation that the Facebook SDK is a technology that is the mobile equivalent of cookies and other technologies that websites use to track visitors and that that are discussed in the opinion. First of all, the Facebook SDK is similar to "social plug-in modules" described in the opinion in that it allows app developers to integrate social plug-ins into their apps, but also contains modules that can be used to track individuals. Secondly, Facebook explicitly equates the tracking of users via "App Events" in the SDK to the use of the Facebook Pixel (a snippet of JavaScript code that allows website to track visitor activity that clearly falls within the scope of ePrivacy). The Facebook Pixel guide on the Facebook developer platform states: "If you want to track User activity in a mobile app, refer to our App Events documentation instead."[72]

The ruling of the Belgian Court against Facebook for its tracking pixel, mentioned above, is thus also highly relevant as this found that Facebook had failed to provide sufficient information and gain consent in breach not just of the Belgian Data Protection law but also the Belgian law implementing the ePrivacy Directive.

Thus, to the extent that the ePrivacy Directive applies (and once the law is updated subject to any changes in the draft Regulation), both further information and valid consent are required.

Competition

Facebook is clearly a dominant player in the third-party tracking market with 42.55 percent of apps[73] on the Google Play store sharing data with Facebook.

Under competition law a dominant player has a 'special responsibility not to allow its conduct to impair genuine undistorted competition in the common market'.[74] This responsibility should be interpreted to prevent companies in dominant position from imposing terms that exclude (or make it more onerous) to offer privacy-friendly services, such as those which do not track individuals' activity.[75] Our research suggests that the default implementation of the Facebook SDK requires app developers to share certain personal data, allowing tracking of users and potentially enabling Facebook to build profiles of individuals. Our research also suggests that a feature that would delay the automated transmission of such data was only available after the GDPR entered into force. This default implementation is a clear obstacle for those app developers which wish to offer privacy friendly (and, potentially, legally compliant) apps to their users buy are relying on the Facebook SDK. It is not sufficient for a company with such market power to simply demand that the app developers comply with their data protection obligations if, at the same

[72] Facebook for developers – Facebook Pixel. Available at: https://developers.facebook.com/docs/facebook-pixel/ (Accessed: 1 December 2018).
[73] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., 2018. Third Party Tracking in the Mobile Ecosystem. arXiv preprint arXiv:1804.03603.
[74] EU Commission guidance 2009/C 45/02
[75] Privacy International (2018). *Competition and Data.* Available at: https://privacyinternational.org/explainer/2293/competition-and-data (Accessed: 1 December 2018).

time, they impose conditions that leave them with no effective alternative between sharing personal data with the dominant company.

Conclusion

Previous research has shown how 42.55% of free apps on the Google Play store could share data with Facebook, making Facebook the second most prevalent third-party tracker after Google's parent company Alphabet.[76] Privacy International's research has illustrated what this data sharing looks like in practice, particularly for people who do not have a Facebook account. We have found that a majority of apps tested share data with Facebook the second the app is launched, and that many apps share quite granular data.

Our research has focused on a small number of these apps, yet the scope of our findings gives reason to believe that a considerable share of apps in the Google play store exhibit similar behavior. In accordance with data protection and ePrivacy law, users must be provided with clear and comprehensive information and provide their consent to such transfer of data to Facebook. Many apps that integrate the Facebook SDK do not appear to provide sufficient transparency or seek consent.

The fact that the SDK's default implementation automatically transmits data when an app is opened, and that a voluntary feature to delay this transmission was only provided in July 2018, raises questions about Facebook's responsibility towards developers, as well as its own compliance with key data protection principles such as data protection by design and by default.

Our findings also show how routinely and widely users' Google ad ID is being shared with third parties like Facebook, making it a useful unique identifier that enables third parties to match and link data about an individual's behavior.

Behavioral advertising in its currently dominant form is driven by a range of invisible tracking technologies, like cookies, device fingerprinting and SDKs, using a variety of techniques, including cross-device tracking and identity matching. Privacy International is greatly concerned about the manifold ways in which people's data is exploited in these hidden back-end systems. Both Google and Facebook are like other ad companies that try to collect a lot of data about what you do online. The crucial difference, however, is that their purview is especially broad.

[76] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., 2018. Third Party Tracking in the Mobile Ecosystem. arXiv preprint arXiv:1804.03603.

Unfortunately, it is difficult to protect yourself from the kind of data sharing that we have described in this report. We have sought to emphasize throughout this report the burden should not be on the individual. That systemic criticism aside, there are some concrete steps that Facebook, Google, app developers, as well as users can take to address some of the concerns we have raised in this report.

Recommendations for Facebook

- Facebook needs to better explain how it uses the data that it automatically receives through the Facebook SDK, how long the data is stored and if it is being shared.
- Facebook should do more to offer products and services that make it as easy as possible for developers to protect the privacy of their users by design and by default. For instance, the default implementation of the SDK should not automatically transmit data the second an app is launched.
- Facebook should take steps to make it easier for people to exercise their data rights on all personal data that Facebook stores, whether they have a Facebook account or not.
- Even though this report has focused on the tracking of non-users, and Privacy International believes that people should always be protected by the highest default settings, Facebook's privacy settings for users are unnecessarily confusing and should be further simplified. It is not clear, for instance, why ad settings are a separate from privacy settings, especially when the former allows people to limit how data that is collected outside the Facebook platform can be used.

Recommendations for Google

- Google should allow users to block third party tracking on Android. The same applies to Apple and iOS.
- Even though the Google ad ID is user-resettable, there is no good reason why the ad ID stays consistent unless a user actively choses to reset their ID. Users should be prompted to reset their ID regularly, for instance, but not limited to when resetting a device to its factory settings. The same applies to the Apple ad ID on iOS.
- Google's privacy settings on Android are confusing and should be simplified. Advertising settings that apply to all apps (such as the ability to reset the Google Ad ID and the ability to limit ad personalization) should not just be hosted under "Google settings" but should be readily accessible under the device's privacy settings. It is counter intuitive that to reset an Ad ID which is used by third parties like Facebook, users have to trawl through Google's settings.

Recommendations for Android developers and app providers

- We are mindful of the fact that many apps are developed by small teams with limited resources. That said, this report has focused on apps that have a user install base in the tens of millions to hundreds of millions. All developers have a responsibility to protect the privacy of their users and comply with existing laws, but this is particularly the case for large apps and those that share unusually granular or sensitive data. Apps should be transparent about third-party tracking on their apps, limit third party tracking to what is strictly necessary and offer users a genuine choice.
- Facebook seeks to place all legal responsibility on app developers and providers. Even though our legal analysis suggests that this is more complicated, we would recommend that app developers think hard about whether their application really needs to use the Facebook SDK, and if they do, use its components selectively, and in a manner that is fair and transparent towards users.

Recommendations for users

- Even if they will not affect the kind of tracking that we have described in this report, we recommend that people make full use of all existing privacy settings, including:
    - Reset your advertising ID regularly – this won't stop you from being tracked and profiled, but it can nonetheless temporarily limit the invasiveness of your profile. This can be found on most Android devices under, Settings > Google > Ads > Reset Advertising ID.
    - Limit ad personalization by opting out of ad personalization in the Android settings. This can be found on most Android devices under, Settings > Google > Ads > Opt out of personalized Advertising.
    - Regularly review the permissions that you have given to different apps and limit them to what it strictly necessary for the way in which you want to use that App. This can be found on most Android devices under, Settings > Apps or Application Manager (depending on your device, this may look different) > tap the app you want to review > Permissions. For example, setting Apps that collect location information, to collect this information not "always" but only "when in use" etc. On recent Android version this is supported natively within the Apps section of settings, on older Android versions App Ops can be used on supported ROMs[i].
    - There are a number of other apps that can be used to control how apps interact with the network and one another. An example is Shelter, which allows you to separate out apps into different profiles within the Android device, allowing for different access controls or

separate Google accounts, allowing separate advertising ID’s to be used for different apps. We haven’t however tested the efficacy of such tools at length

- The addition of a phone-based firewall can also be used to limit connections to addresses such as graph.facebook.com. Examples such as AFWall+ or NetGuard. We would suggest users conduct their own research before using such tools and understand their limitations and ramifications.

Appendix

Appendix 1 – Summary of Apps tested

All apps were tested between August and December 2018, with the last re-test happening between 3 and 11 of December 2018. The full documentation, including the exact date each app was tested, the SDK version used, as well as the data transmitted can be found here: privacyinternational.org/appdata

By size of install base and popularity

	Install base	Genre	Observation 1	Observation 2
Dropbox	>500,000,000	PRODUCTIVITY	No	No
Super-Bright LED Flashlight	>500,000,000	PRODUCTIVITY	Yes	No
My Talking Tom	>500,000,000	GAME_CASUAL	Yes	No
Skater Boy	>100,000,000	GAME_ARCADE	Yes	No
Tripadvisor	>100,000,000	TRAVEL_AND_LOCAL	Yes	No
Shazam	>100,000,000	MUSIC_AND_AUDIO	Yes	No
Spotify	>100,000,000	MUSIC_AND_AUDIO	Yes	No
Candy Crush	>100,000,000	GAME_CASUAL	No	No
Indeed Job Search	>50,000,000	BUSINESS	Yes	No
Duolingo	>50,000,000	EDUCATION	Yes	Yes

	Install base	Genre	Observation 1	Observation 2
Skyscanner	>10,000,000	TRAVEL_AND_LOCAL	Yes	Yes
Yelp	>10,000,000	TRAVEL_AND_LOCAL	Yes	No
Kayak	>10,000,000	TRAVEL_AND_LOCAL	Yes	Yes

By size of install base, non-English userbase

	Install base	Genre	Observation 1	Observation 2
WeChat	>100,000,000	COMMUNICATION	No	No
VK	>100,000,000	SOCIAL	Yes	No

By category, health and fitness

	Install base	Genre	Observation 1	Observation 2
Period Tracker - Period Calendar Ovulation Tracker	>50,000,000	HEALTH_AND_FITNESS	No	No
Calorie Counter – MyFitnessPal	>50,000,000	HEALTH_AND_FITNESS	Yes	No
Instant Heart Rate: Heart Rate & Pulse Monitor	>10,000,000	HEALTH_AND_FITNESS	No	No
BMI Calculator and weight tracker	>10,000,000	HEALTH_AND_FITNESS	No	No
Period Tracker Clue:	>10,000,000	HEALTH_AND_FITNESS	Yes	No

By category, lifestyle

	Install base	Genre	Observation 1	Observation 2
The Bible	>100,000,000	LIFESTYLE	No	No
Muslim Pro - Prayer Times, Azan, Quran & Qibla	>10,000,000	LIFESTYLE	Yes	No
Salatuk (Prayer Time)	>10,000,000	LIFESTYLE	Yes	No
Family Locator GPS Tracker	>10,000,000	LIFESTYLE	Yes	No
Phone Tracker By Number	>10,000,000	LIFESTYLE	No	No
King James Bible	>10,000,000	LIFESTYLE	Yes	Yes
Qibla Connect	>10,000,000	LIFESTYLE	Yes	No

By category, utility and communication

	Install base	Genre	Observation 1	Observation 2
Security Master	>500,000,000	TOOLS	Yes	No

	Install base	Genre	Observation 1	Observation 2
Turbo Cleaner	>100,000,000	TOOLS	TBD	TBD
Speedtest.net	>50,000,000	TOOLS	No	No
Clean Master	>50,000,000	TOOLS	Yes	No
HP ePrint	>10,000,000	PHOTOGRAPHY	No	No
Opera	>100,000,000	COMMUNICATION	No	No

Appendix 2 – Company responses

Privacy International has given Facebook, Google and all apps for which we observed our findings an advance notice of this report on 19 December 2018. For the purpose of accuracy, we provided companies with the opportunity to respond to queries related to the key statements we planned to make. We believe these statements to the best of our knowledge to be true and accurate.

Skyscanner, 22 December 2018 (via E-Mail to Privacy International)

"Many thanks for alerting Skyscanner to this issue. Our goal is to be as transparent and upfront as possible with travellers regarding what information is collected from them and who it is shared with. Since receiving your letter, we released an update to our app as a priority which will stop the transmission of data via the Facebook SDK. As a further result of this we will audit all our consent tracking and are committed to making any changes necessary to ensure that travellers privacy rights are fully respected."

TripAdvisor, 24 December 2018 (via E-Mail to Privacy International)

"We write in response to your letter dated 19 December 2018 in which you provide advance notice of a publication regarding third party tracking via the Facebook SDK on Android applications. […] In addition to providing acknowledgement of receipt, we write to advise that we are committed to engaging with Privacy International. Respecting the data protection rights of our users is of utmost importance to

TripAdvisor. […] Given the complexity of the technical issues you raise, we respectfully consider the statements you have made to be somewhat oversimplified. […]"

My Fitness Pal (Under Armour), 26 December 2018 (via E-Mail to Privacy International)

"Thank you for reaching out regarding our data privacy practices and program. The SDK identified is a common analytics tool. It provides information that allow apps, like MyFitnessPal, to improve the services provided to their user communities (i.e., it serves to provide an aggregative view of app installs, app open, and in app purchase activity – information that is then used to enhance the app experience). MyFitnessPal specifically outlines this to users in its Privacy Policy as analytics processed for a legitimate interest as permitted under Art. 6 (1) (f) of the General Data Protection Regulation (GDPR), namely "… to enhance … [user] experience and to develop and improve our Services." We trust this explanation responds to your inquiry. Please let us know if you have any follow up questions."

My Talking Hank and My Talking Tom (Outfit7), 27 December 2018 (via E-Mail to Privacy International)

"Thank you for taking the time to review our privacy practices. We take the privacy of our users very seriously, so we're glad to have the chance to cooperate with Privacy International.

To demonstrate our commitment to the privacy of our users, we've undergone the robust certification process for compliance with the GDPR and we're also members of the ePrivacyApp certification program (the "Program"). ePrivacy is an independent, third-party organization specializing in digital data protection. As part of the Program, Outfit7's Talking Tom and Friends and other characters applications are subject to a comprehensive inspection and certification of the applications with respect to ensure that the applications live up to the high demands in the field of data protection and can provide a high level of security of end user data.

Please note that we are aware of the problem with Facebook SDK and we have been actively working on finding solutions to ensure privacy of our end user data. Please see exhibit A - Jira Ticket - which clearly shows that we started working on updating Facebook SDK already in September, 2018 in order to ensure that end user data is being collected in compliance with the law. For the EEA territory, which includes UK, the internal instructions were, that all app events, together with the advertising ID, sent to graph.facebook.com must be disabled for users that are below 16 or do not pass the localized age gate (meaning age gate, which is set in accordance with the local legislation regarding the year of consent). For users that are above 16 or pass the localized age gate, Facebook login SDK must be added to our consent tool and no app event data (including advertising ID), should be sent to graph.facebook.com *unless user gives consent. On October 17, 2018, we have decided to **entirely disable transmission of app events data (including advertising ID) to graph.facebook.com regardless of the fact whether user passed the age gate or not.** Please note that in order for us to update Facebook SDK in a particular app, the app needs to be updated, which was done in a regular course of updates. The first app that was updated with the updated Facebook SDK was Talking Tom Gold Run (November 20, 2018). My Talking Tom and My Talking Angela apps were updated on December 20, 2018. All the other apps, including My Talking Hank, will get updated by the end of February 2019."*

The Weather Company, 27 December 2018 (via E-Mail to Privacy International)

"The Weather Channel (TWC) is committed to protecting user privacy, which includes empowering the user to choose whether to receive personalized advertising. The current version of the TWC Android app — released globally on December 10 — does not utilize the Facebook Login SDK referenced in your December 19, 2018, letter. TWC encourages its users to use the most up-to-date version of the app in order to maximize their user experience and privacy protections."

VK, 27 December 2018 (via E-Mail to Privacy International)

"VK apps use standard Facebook Login, Sharing and Core SDKs to provide VK users the ability to find friends from Facebook and share their VK content. In particular, VK:

- provides users the ability to log in into VK app via their Facebook account (FB OAUTH),

- allows users find their Facebook friends on VK,

- provides users the ability to share VK posts and videos on their Facebook account.

All of this is disclosed in our Privacy Policy: https://vk.com/privacy/eu

We do not use the data transmitted via Facebook SDKs for any analytical or tracking purposes."

Spotify, 27 December 2018 (via E-Mail to Privacy International)

"Thank you for bringing this matter to our attention. Spotify is committed to transparency and fairness in how it processes personal data in connection with the Spotify app and service. We are currently working to evaluate Privacy International's technical findings (the details of which shared by Privacy International are quite brief) and to understand the context of data being transmitted to graph.facebook.com. If necessary, we will also evaluate whether changes should be made as part of this

Facebook integration. However, as this is a technically complex and important matter, our technical evaluation is unlikely to be complete prior to your organisation's publication of its report."

Google, 28 December 2018 (via E-Mail to Privacy International)

"The behavior described in the paragraph above would be the result of a sharing arrangement between Facebook and a third-party app developer. This sharing arrangement could work like this: the developer would have included Facebook code in their application, and that code would report back to Facebook. This sharing arrangement does not involve Android. The behavior described is not Android behavior, is not specific to Android, and it does not occur as a result of any aspect of Android's design. The same behavior will be observed in other operating systems because it is the byproduct of Facebook's arrangements with the third-party apps that implement Facebook's SDK.

Google: *All Android devices running Google Play will have an Advertising ID generated on the device. There are controls that allow users to reset the Advertising ID at any time, for any reason. Users cannot remove the Advertising ID completely: Advertising ID allows applications and advertising networks to measure clicks without resorting to more intrusive forms of identification, such as phone number, SSAID or device fingerprint, which users cannot reset. It also serves to combat advertising fraud.*

Privacy International: 3. Google allow users to reset (and thereby change) their Advertising ID in their phones' Google settings. However, we found that unless a user actively changes their Advertising ID, it stays persistent. For instance, we found that the Advertising ID doesn't change when a device is reset to its factory settings if the user logs in using the same Google account.

Google: *"This is inaccurate. We would expect that a factory reset of the device would have the effect of generating a new Advertising ID. We tested a couple of devices we had on hand, and confirmed that the Advertising ID was changed upon factory reset, regardless of whether the user signed in with the same Google account or not. If you are seeing other behavior, it would be useful to know the precise specifications of the device and version of Android. In general, the Advertising ID does remain the same until it is reset by the user — which the user can do at any time for any reason."*

Privacy International: 4. Devices running Android 6.0 and up afford users control over some of the data that each app is permitted to collect. These settings, however, cannot control the automatic transmission of the data via the Facebook SDK.

Google: *As described above, the transmission of data between a third-party app and Facebook via the Facebook SDK is the result of the sharing arrangement between the app developer and Facebook. This behavior is not specific to Android nor the result of any aspect of Android's design.*

Privacy International: 5. Google also allows users to "Opt out of Ads Personalization" on Android. While this allows users to opt out of ad personalization across Google ads services (ex: Search ads) and the 2+ million websites and apps that partner with Google to show ads, it does not mean that users opt out of third-party tracking.

Google: *"This is inaccurate. If a user disables "ads personalization" in the device Advertising ID settings, no app or ad vendor may use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising. This is true for Google apps, like Google Search, Maps and YouTube, but it is also true for all other apps installed on the device. This requirement is established via the Play Developer terms.*

Separately, Google users can disable ads personalization via a control in the Google Account controls. This will stop Google advertising services from creating user profiles for advertising purposes or for targeting users with personalized advertising. Opting out of ads personalization via the Google Account control will automatically apply on any device where the user signs in to his or her Google account."

Facebook, 28 December 2018 (via E-Mail to Privacy International)

Dear [Privacy International],

[…] Thank you again for the opportunity to review and respond to the findings of an investigation Privacy International has conducted regarding third party tracking via the Facebook SDK on Android apps. These are important issues that you've raised and we share your goal of ensuring that Privacy International's assessment is as accurate as possible. Because we have not been provided with a copy of the full report, we are responding only to the sections we received several days ago. We look forward to providing additional responses once you're able to share the final report with us after it's published.

We hope the information we provide below is helpful, and wanted to share a link to a blog post we published earlier this year that provides additional information on how Facebook uses data that comes from other websites and apps: https://newsroom.fb.com/news/2018/04/data-off-facebook/. We also wanted to note that many companies offer the types of services you cover in the report and, like Facebook, they also get information from the apps and sites that use them in a similar manner. Amazon, Google and Twitter all offer login features. Likewise, many of these companies, as well as others like Adobe, Flurry, and Mixpanel, provide analytics services for app developers. More generally, most websites and apps send the same information to multiple companies each time you visit them.

As we explain in more detail below, developers can choose to collect app events automatically, to not collect them at all, or to delay collecting them until consent is obtained, depending on their particular *circumstances. We also require developers to ensure they have an appropriate legal basis to collect and process users' information. Finally, we provide guidance to developers on how to comply with our requirements in this regard.*

We agree that, as you point out, it's important for people to have access when we receive information about them when they're not using our services, and to have control over whether we associate this information with them. Recognizing the value of improvements in this area, we're currently working on a suite of changes, including developing a new tool called Clear History, that we hope will address your feedback.

Our responses to your questions, below, reflect our current practice and what we understand to be industry-standard. As noted, we're also actively working on improved functionality that we hope will lead the industry — and we'd be grateful for your feedback as we develop our approach.

Privacy International: 1. As Facebook explains in its UK privacy policy, app developers transmit data to Facebook through the Facebook SDK. 1

Facebook: *"In our Data Policyand Cookies Policy, Facebook Ireland explains how it receives data collected by advertisers, app developers and publishers via the Facebook SDK. We ensure that these policies are accessible from each page on Facebook, and that users can access and read these policies when they sign up to Facebook or during updates to these policies.*

For example, in our Data Policy, we explain:

Information from partners.

Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.

To learn more about how we use cookies in connection with Facebook Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

As we mention above, this is common industry practice and others offer similar information notices about their services."

Privacy International: 2. Using the free and open source software tool called "mitmproxy", an interactive HTTPS proxy, Privacy International analyzed the data that a number of Android apps transmit to Facebook through the Facebook SDK. We found that the majority of the apps we tested transmit data to graph.facebook.com the second the app is opened. Typically, the first data that is automatically transmitted is events data that communicates to Facebook that the Facebook SDK has been initialized by transmitting events data such as "App installed" and "SDK Initialized", together with the user's Google advertising ID. Since the data is transmitted immediately, users are unable to agree or give consent.

Facebook: *"Facebook offers analytics and advertising services to app developers, which help them receive aggregated information about how people engage with their apps — this is a common practice for many companies. This information is important for helping developers understand how to improve their apps and for helping people receive relevant advertising in a privacy-protective way. We do this in a transparent manner by explaining the practice through our Data Policy and Cookies Policy, and by using Google's advertising identifier, which can be controlled centrally by people using their device settings.*

EU data protection law and data protection authorities have made clear that the company who is the "data controller" of an individual's personal data is responsible for having the right legal basis to collect and process that individual's personal data. In addition, we require developers to confirm that they've gotten consent from their users to send information to Facebook (via Section 3(c) of our Business Tool Terms), and we also provide guidance about how to implement consent mechanisms. For example, in our Business Tool Terms we state:

In jurisdictions that require informed consent for the storing and accessing of cookies or other information on an end user's device (such as but not limited to the European Union), you must ensure, in a verifiable manner, that an end user provides the necessary consent before you use Facebook Business Tools to enable us to store and access cookies or other information on the end user's device. (For suggestions on implementing consent mechanisms, visit Facebook's Cookie Consent Guide for Sites and Apps.)

Where Facebook Ireland processes the data as a data controller-- for example for safety, integrity and security purposes, or to personalise the ads the Facebook user sees— we are responsible for ensuring *compliance with the GDPR and for having a valid legal basis to legalise this processing. Facebook ensures it has a valid legal basis or bases to support all these processing purposes. For example, we collect consent from individuals to use data collected from partners to personalise the ads they see — and we don't use data in this way if they do not consent."*

Privacy International: 3. This automatic transmission of data is the default implementation of the Facebook SDK. This is clearly stated in Facebook's Analytics Quickstart Guide for Android, which states: "When you use the Facebook SDK, some events in your app are automatically logged and collected for Facebook Analytics unless you disable automatic event logging." 2

Facebook: "*An app developer can get a user's consent to collect and process their data (including sending it to Facebook via the SDK). They can also choose to disable automatic event logging. Earlier this year, we also introduced a new option that allows developers to delay collection of app analytics information.*

First and foremost, we want to make sure developers understand that, under EU data protection law, the company who is the "data controller" of an individual's personal data (the app developer in this case) is responsible for having a valid legal basis to collect and process an individual's personal data— so we require developers to provide "robust and sufficiently prominent notice" to their users regarding the collection, sharing and usage of their data (Section 3(b) of our Business Tools Terms) as well as, where required (for example to comply with the ePrivacy rules), obtain necessary end user consent before sending us data via our SDK (Section 3(c) of our Business Tools Terms).

Our developers are able to choose how they meet this contractual obligation, but must meet the obligation. And of course they are responsible for their own obligations under the law, which can be enforced by data protection authorities. For example, a developer could choose to make an appropriate in-time pre-install disclosure— such as by obtaining consent from users during a registration flow (where users have to create an account and accept terms before using the website or app). This way, they can ensure that their users have given appropriate permission for their personal data to be sent to Facebook via the SDK.

If an app developer chooses not to use a registration flow to get a user's consent for auto-event logging, or if for any reason they're unable to get prior consent via another pre-install mechanism, they can always disable to auto-log feature (as you note above in your statement)."

Privacy International: 4. Facebook only released a voluntary SDK feature that allows app developers to delay collecting automatically logged events until they acquire user consent on June 28, 2018. 3

Facebook: *"Yes; as explained above, in June of this year we introduced another option for businesses that want to use our auto-event logging feature if they choose not to use a pre-install mechanism for obtaining the prior consent contractually required. The legal and contractual obligation is on the developer (data controller) to get consent as required from their users before sharing personal data with Facebook via the SDK, and we wanted to provide another tool in the toolbox to help developers fulfill their legal and contractual obligations, while also providing a good experience for their users.*

Privacy International: 5. Before that date it was impossible for Apps to delay transmitting data to Facebook when using the Facebook SDK.

Facebook: *"Prior to our introduction of the "delay" option, developers had the ability to disable transmission of automatic event logging data, except for a signal that the SDK had been initialized. Following the June change to our SDK, we also removed the signal that the SDK was initialized for developers that disabled automatic event logging.*

In June we also introduced another option for businesses that want to use our auto-event logging feature in compliance with our Business Tools Terms. Today, an app developer can either choose to use a pre-installed mechanism for obtaining an end-user's prior informed consent (as they could in the past), or use the SDK delay feature."

Privacy International: 6. Without any further transparency from Facebook, it is impossible to know for certain, how the data that we have described in this report is being used. Facebook's business tools terms describe a number of additional uses of "event data", that is the data that we have described throughout this report: 4 The uses described in Facebook's business tools terms depend on the kind of Facebook Company Product apps and websites chose to use. The SDK contains a number of core components: Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links and apps can choose to use these features selectively. Since the data transmission we have observed in this report, however happens automatically and this independently from the component that an app uses, it is unclear which uses apply.

Facebook: *"We do want to make sure that we are transparent about the data we collect and use. Our Data Policy(which is our primary privacy notice) and Cookies Policydescribes the ways in which we collect data and the uses for which we may process that data, including how we use data from partners. For example, Facebook provides users the ability to authenticate with third-party apps in an easier way* *through Facebook Login product. Developers can receive analytics that allow them to understand what the audience of their app enjoys and improve their apps over time. Developers may also use Facebook services to monetise their apps through Facebook Audience Network. Subject to that Facebook user's prior consent, Facebook may also use this data to provide that user with more personalised ads."*

Privacy International: 7. Developers have filed bug reports about the SDK transmitting data even when disabling auto events in August 5, October 6and November 7of 2018. This raises the question whether the voluntary feature that was released on June 28, 2018 works in practice.

Facebook: *"The voluntary feature that we released on June 28, 2018 for the Android SDK worked as we described at the time of launch. Following the launch, we received feedback from developers and made changes to (1) expand the information that we did not collect during the delay period, and (2) make the delay functionality available in our Unity SDK, which is separate from the Android SDK."*

Privacy International: 8. On October 29, 2018, Christopher Weatherhead, a member of staff, submitted an access request via the online form that Facebook provides for non-users of its platform 8, requesting access to all personal data relating to the Google advertising ID that was used in conducting this research. The rationale behind this access request was to gain further understanding about the ways in which Facebook uses the data it receives from apps and for how long it is being stored. Facebook auto responded on October 29, 2018, asking the user to confirm that they don't have a Facebook account, asking whether the users has had a previous account associated with their email address, as well as a detailed explanation of the information the user is requesting. On October 29, 2018 the member of staff confirmed that their email address is not (and has never been) associated with a Facebook and requested all personal data that is associated with their Google Advertising ID. On October 30, 2018 Facebook responded: "we couldn't find a Facebook account associated with the email address you're using to contact us. If you have a Facebook account associated with a different email address, please submit a new report." On November 29, 2018 the member of staff sent a reminder. On December 6, 2018, the staff member sent another reminder. We would be grateful if you could respond to the access request by Christopher Weatherhead.

Facebook: *"Thank you for following up with us on Mr Weatherhead's access request. We have replied to Mr Weatherhead regarding his request and are happy to continue communication with him should he wish to do so. All communication regarding access requests takes place directly with the data subjects concerned*