Major Android apps are still sending data directly to Facebook to spy on you

comments

Even when you’re not logged in or don’t have a Facebook account

By Nick Statt@nickstatt

Share

Illustration by Alex Castro / The Verge

Major Android mobile apps from companies including Yelp and Duolingo send data that could be used to personally identify you for ad tracking straight to Facebook immediately upon logging in, according to a new report from the London-based UK charity and watchdog group Privacy International (PI). This data transfer happens even if a user isn’t logged into Facebook on that device and even in the event the user doesn’t have an active Facebook account at all.

In addition to Yelp and Duolingo, PI found that two Muslim prayer apps, as well as a bible app and a job search app called Indeed, also sent similar data to Facebook that could be used to help identify users for ad targeting purposes when they browse the social network. It’s not clear exactly what type of data is being sent in this case, other than that a user opened the app at a given time, but PI’s report says this transmission may also reveal custom identifiers that help Facebook track that user

across its network of services and when that person opens Facebook on a mobile device.

The report builds on a similar investigation from PI last December that first revealed that big-name Android apps were sending data to Facebook without a user's consent and without proper disclosure. It also highlights that this problem is universal across both iOS and Android; last month, *The Wall Street Journal* revealed that these same set of developer tools that scrape data when you use a mobile app and send it to Facebook are employed on iPhone apps, despite Apple's much more stringent privacy rules and protections.

"This is hugely problematic, not just for privacy, but also for competition. The data that apps send to Facebook typically includes information such as the fact that a specific app, such as a Muslim prayer app, was opened or closed," reads PI's report, published earlier today. "This sounds fairly basic, but it really isn't. Since the data is sent with a unique identifier, a user's Google advertising ID, it would be easy to link this data into a profile and paint a fine-grained picture of someone's interests, identities and daily routines."

> Bad news: @Yelp @indeed a Bible app and two Muslim prayer apps still send your personal data to Facebook before you can decide whether you want to consent or not… ♀ ♀ ♀
> These are apps with millions of installs!https://t.co/I7pGQFD2jR (2/6)
> pic.twitter.com/pQx3bMV1YH
>
> — Privacy International (@privacyint) March 5, 2019

As Facebook's privacy practices come under even greater scrutiny in the aftermath of last year's Cambridge Analytica data privacy scandal, a spotlight is being shone on the lesser-known arrangements between large advertising companies and the smaller app makers that use those platforms to reach new users and target existing ones with ads. As revealed by *the WSJ* last month, a number of prominent iOS app makers use a Facebook analytics tool known as "custom app events" that, in this case, was sharing sensitive health, fitness, and financial data with the social network for ad targeting purposes.

On Android, Facebook has long collected sensitive user data such as contact logs, call histories, SMS data, and real-time location data, for the purpose of informing its ad targeting and improving features like friend suggestions. Yet the practices have caused vocal outcry from privacy advocates and users concerned Facebook is amassing far too much data about their personal lives and online and offline behaviors. Following reports about Facebook using its location-tracking capabilities to catch company interns skipping work, it said it would allow Android users the ability to explicitly disable the feature.

In this case, PI is underscoring one of Facebook's longstanding indirect data collection policies, one that relies on third-party apps to autonomously collect and send information about app usage to the social network without telling users about the arrangement.

"App makers send information about users straight to Facebook, often without consent or disclosure"

"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," PI explained in the initial December 2018 report. The report found that nearly two thirds of the 34 Android apps PI tested — including big names like Spotify and Kayak and all of which had between 10 and 500 million installs — sent information to Facebook without informing users or gaining express consent.

PI says that a number of apps stopped the practice following its December report. Similarly, most of the operators of the iOS apps highlighted in the *WSJ* report also ceased using Facebook's analytics and developer tools to collect sensitive user data. However, it appears some apps, like Yelp's and Duolingo's, continue to do so. PI says it's in contact with Duolingo, and the company has agreed to suspend the practice, but it's not clear how many other apps in the Android or iOS ecosystem may be skirting Apple and Google's data-collection and user privacy policies to improve Facebook's ad targeting tools.

In these situations, Facebook puts the onus on app makers not to break platform rules or misuse its developer tools by collecting sensitive information. The company has also claimed not to use a majority of this sensitive data and, in some extreme cases like credit card numbers and Social Security numbers, automatically deletes it. But it's not clear why the data is being collected in the first place and what ways it's been put to use in the past, either by the apps collecting it or by Facebook.

"Apps relay on the Facebook SDK to integrate their product with Facebook services, like Facebook's login and ad tracking tools.

However, Facebook places all responsibility on apps to ensure that the data they send to Facebook has been collected lawfully," reads PI's report. Facebook not immediately available for comment.