How Facebook was able to siphon off phone call and text logs
By RYAN NAKASHIMA and MAE ANDERSON
Associated Press, Mar. 27, 2018

The news that Facebook's Android app has been collecting call and text histories is yet another black eye for the social media giant. But just why was Facebook able to siphon off records of who its users were contacting — and when — in the first place? The short answer: Because Google let it. The longer answer: Well, it's complicated.

The social network acknowledged on Sunday that it began uploading call and text logs from phones running Google's Android system in 2015 — first via its Messenger app and later through an option in Facebook Lite, a stripped-down version of its main app. Facebook added that only users who gave appropriate permission were affected, that it didn't collect the contents of messages or calls, and that users can opt out of the data collection and have the stored logs deleted by changing their app settings.

Facebook did not respond to multiple requests for more specifics. The kerfuffle over this data collection, first reported by the website Ars Technica , follows a week of turmoil for the social network involving charges that it allowed political consultants to steal the data of 50 million users in order to influence elections.

There's a reason Facebook's actions were restricted to Android phones. Apple locks down app permissions tightly, which offers more privacy protection to iPhone users. "Apple's fundamental approach is to collect the minimum amount of information to keep the service running, and keep customers in control of the information," said Rich Mogull, CEO of the security firm Securosis.

But Android has long been more indulgent.
Until recently, in fact, Google let app developers gain access to a phone's call and text logs. All they needed was an app that required access to user contacts. Once users agreed, Android would then also grant access to those communication histories.

Starting in 2012 with its "Jelly Bean" release, Android would notify people installing such apps that they were also giving apps access to their call and text logs, but still required them to agree to all those permissions at once. Rejecting the request meant the apps wouldn't work.

It wasn't until 2015 when Google released Android 6.0, dubbed "Marshmallow," that Android phones finally split up those permissions. That meant users could agree to share contacts, but reject access to their messaging and phone histories.

That's the same year Facebook says its apps started collecting this information. But many Android users aren't using the latest version of the software. In fact, they often can't get it even if they want it.

Apple owns both the software and hardware for iPhones, which allows it to push out new versions of its iOS operating software at will. Google, by contrast, is largely at the mercy of both mobile carriers and hardware makers when it comes to distributing new Android versions.

There are nearly 20,000 Android phone models now in service, and carriers like to tweak the software for each to ensure that it will work as smoothly as possible on their networks. As a result, new Android versions reach users very slowly.

As of January, about 65 percent of iPhone users were using the latest iOS software, introduced in 2017. Less than 1 percent of Android devices currently use the latest version of Android, known as "Oreo." (Many of them are owners of Google's new Pixel phones, which get software updates directly from Google.)

Just over half of all Android users are using the two previous versions, which allow them to specifically reject the sharing of communication logs. Last October, Google began forcing all apps to follow the new rules when they issue updates, even on phones running older versions of Android.

All that leaves two big questions unanswered. Why did Google set up Android permissions this way? And how many other apps have taken advantages of the same setup?

Experts and privacy advocates say the answer to the first question is probably related to Google's advertising-based business model, which — like Facebook — depends on collecting detailed information about users in order to target them with tailored ads. Apple, meanwhile, derives its profits from the sale of devices and services like Apple Music.

Another possible factor: Android was playing catch-up with Apple for many years, and was eager to attract app developers in order to attain parity with Apple's App Store. Some app developers may have found greater access to user data on Android attractive — as Facebook did.

Experts say it's not clear if other apps are going as far as Facebook in terms of tracking call history and texts, but it's very possible.

"In a lot of ways, Facebook is the tip of the iceberg," said Bob O'Donnell, chief analyst at Technalysis Research. "There are plenty of other people doing this kind of data collection."

It is unclear how many apps gained access to call logs so far or how many users' call logs had been sent to app developers. A Google spokesperson declined to comment.

One major Android phone maker expressed uncertainty over its role in protecting user privacy. "At this time the nature of the data breach is unclear so it is difficult to comment on the cause or the solution," LG Electronics Inc. said Tuesday in a statement.

___

AP Technology Writer Youkyung Lee in Seoul, South Korea, contributed to this report.