PHYS ORG

The difficulty of determining which internet apps track personal data

May 24 2017, by Suranga Seneviratne And Dali Kaafar

Both paid and unpaid apps can track your data. The apps pictured may not - but it’s hard to know which do and which don’t. Credit: Flickr/Blake Patterson, CC BY-SA

Anyone who spends much time online knows the saying: "If you're not paying, you're the product". That's not exactly correct.

On the internet, you're nearly always the product. And while most internet users know that some of their personal data is being collected and monetised, few are aware of the sheer scale of the issue, particularly when it comes to apps.

In fact, our research suggests a majority of the top 100 paid and free Google Play apps in Australia, Brazil, Germany and the US contain at least one tracker. This means data could be collected for advertising networks as well as for payment providers.

This is just the beginning. As voice-activated intelligent assistants like Siri or Google Now evolve and replace the need for apps on our smartphones, the question of what is being done with our data will only grow more complicated.

Nothing is free

The difference between what apps actually do with user data and what users expect them to do was apparent in the recent Unroll.Me scandal.

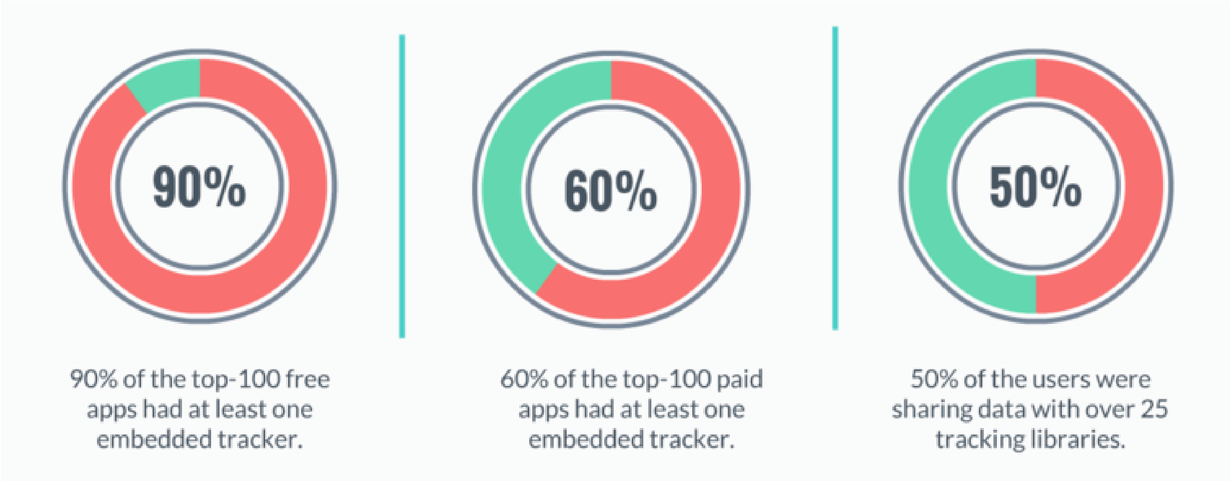
Unroll.me is a free online service that cleans email inboxes by unsubscribing the user from unnecessary emails. But many were dismayed when the company was recently discovered to be monetising their mail content. For example, UnRoll.me was reportedly looking for receipts of the ridesharing company Lyft in user emails and selling that information to Uber.

Unroll.me's CEO apologised, saying the company needed to do a better job of disclosing its use of data. But who is in the wrong? Consumers for thinking they were getting a service for free? Or the service provider, who should inform customers of what they're collecting?

The question is even more intriguing when it comes to mobile apps.

In fact, compared to online services that usually access a few facets of a user's personal profile, mobile apps can conveniently tap into a range of personal data such as location, message content, browser history and app installation logs.

They do this using third-party libraries embedded in their code, and these libraries can be very intrusive.



A summary of the study of top-100 free and paid apps in Google Play Store. Credit: NICTA, Author provided

How libraries work

Libraries are third-party trackers used by app developers so they can integrate their products with external services. These may include advertising networks, social media platforms and payment gateways such as Paypal, as well as tools for tracking bugs and crashes.

In our study, carried out in 2015, we analysed tracking libraries in the top-100 free and top-100 paid apps in in Australia, Brazil, Germany and the US, revealing some concerning results.

Approximately 90% of the top free apps and 60% of the top paid apps in Google Play Store had at least one embedded tracker.

For both free and paid apps in the study, Google Ads and Flurry were the two most popular trackers and were integrated with more than 25% of the apps. Other frequently observed libraries include Chartboost, Millennial Media, Google Analytics and Tapjoy. The top trackers were also likely to be present in more than one app, meaning these libraries receive a rich dataset about the user.

Of course, these numbers could have changed in the two years since our research was published, although recent studies suggest the trend has largely continued.

It's also possible these libraries are present without collecting data, but it's nonetheless disturbing to see the presence of so many trackers in paid apps that have an alternative business model.

What lies ahead?

So what can you do if you don't want to be tracked?

- Use your judgement when giving apps permission to access your data by first asking questions such as, "does this game really need to know my phone number?"
- Consider using mobile anti-virus and privacy advisory apps such as Lookout Security & Antivirus, Mobile Security and Antivirus, and PrivMetrics (this app is a beta release by Data61).

Ultimately, however, these solutions barely touch the surface of a much larger issue.

In the near future, apps may be replaced by built-in services that come with a smartphone's operating system. The intelligent personal assistant by Google, Google Now, for example, could eliminate the need for individual transport, messenger, news and weather apps, as well as some financial apps.

These services, otherwise known as aggregator platform services, could build extensive profiles that cover several aspects of our online and offline behaviour. When used, they have access to an incredibly broad range of our activities, not to mention our location.

Still, app users have so far been willing to exchange their data for convenience. There's little reason to believe that trend will not continue.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: The difficulty of determining which internet apps track personal data (2017, May 24) retrieved 26 April 2024 from https://phys.org/news/2017-05-difficulty-internet-apps-track-personal.html