ANDROID USERS: TO AVOID MALWARE, TRY THE F-DROID APP STORE

The scourge of hidden trackers in Android apps means users should stop using the Google Play store, researchers argue. BADBROTHER/GETTY IMAGES

IN THE EARLY days of Android, co-founder Andy Rubin set the stage for the fledgling mobile operating system. Android's mission was to create smarter mobile devices, ones that were more aware of their owner's behavior and location."If people are smart," Rubin told Business Week in 2003, "that information starts getting aggregated into consumer products." A decade and a half later, that goal has become a reality: Android-powered gadgets are in the hands of billions and are loaded with software shipped by Google, the world's largest ad broker.

IRED
PINION

)'Brien and Michael
re visiting fellows at
y Lab
ePrivacyLab), an
ve of the Information
y Project at Yale Law

Our work at Yale Privacy Lab, made possible by Exodus Privacy's app scanning software, revealed a huge problem with the Android app ecosystem. Google Play is filled with hidden trackersthat siphon a smörgåsbord of data from all sensors, in all directions, unknown to the Android user.

As the profiles we've published about trackers reveal, apps in the Google Play store share a

. Contact
ecurely.

wide variety of data with advertisers, in creative and nuanced ways. These methods can be as invasive as ultrasonic tracking via TV speakers and microphones. Piles of information are being harvested via labyrinthine channels, with a heavy focus on retail marketing. This was the plan all along, wasn't it? The smart mobile devices that comprise the Android ecosystem are designed to spy on users.

One week after our work was published and the Exodus scanner was announced, Google said it would expand its Unwanted Software Policy and implement click-through warnings in Android.

But this move does nothing to fix fundamental flaws in Google Play. A polluted ocean of apps is plaguing Android, an operating system built upon Free and Open-Source Software (FOSS) but now barely resembling those venerable roots. Today, the average Android device is not only susceptible to malware and trackers, it's also heavily locked down and loaded with proprietary components—characteristics that are hardly the calling cards of the FOSS movement.

Though Android bears the moniker of open-source, the chain of trust between developers, distributors, and end-users is broken.

Google's defective privacy and security controls have been made painfully real by a recent investigation into location

tracking, massive outbreaks of malware, unwanted cryptomining, and our work on hidden trackers.

The Promise of Open-Source, Unfulfilled

It didn't have to be this way. When Android was declared Google's answer to the iPhone, there was palpable excitement across the Internet. Android was ostensibly based on GNU/Linux, the culmination of decades of hacker ingenuity meant to replace proprietary, locked-down software. Hackers worldwide hoped that Android would be a FOSS champion in the mobile arena. FOSS is the gold-standard for security, building that reputation over the decades because of its fundamental transparency.

As Android builds rolled out, however, it became clear that Rubin's baby contained very little GNU, a vital anchor that keeps GNU/Linux operating systems transparent via a licensing strategy called copyleft, which requires modifications to be made available to end-users and prohibits proprietary derivatives. Such proprietary components can contain all kinds of nasty "features" that tread upon user privacy.

As a 2016 Ars Technica story made clear, there were directives inside Google to avoid copyleft code—except for the Linux kernel, which the company could not do without. Google preferred to bootstrap so-called permissively licensed code on top of Linux instead. Such code may be locked down and doesn't require developers to disclose their modifications—or any of the source code for that matter.

Google's choice to limit copyleft's presence in Android, its disdain for reciprocal licenses, and its begrudging use of copyleft only when it "made sense to do so" are just symptoms of a deeper problem. In

an environment without sufficient transparency, malware and trackers can thrive.

Android's privacy and security woes are amplified by cellphone companies and hardware vendors, which bolt on dodgy Android apps and hardware drivers. Sure, most of Android is still open-source, but the door is wide open to all manners of software trickery you won't find in an operating system like Debian GNU/Linux, which goes to great length to audit its software packages and protect user security.

Surveillance is not only a recurring problem on Android devices; it is encouraged by Google through its own ad services and developer tools. The company is a gatekeeper that not only makes it easy for app developers to insert tracker code, but also develops its own trackers and cloud infrastructure. Such an ecosystem is toxic for user privacy and security, whatever the results are for app developers and ad brokers.

Apple is currently under fire for its own lack of software transparency, admitting it had slowed down older iPhones. And iOS users should not breathe a sigh of relief in regard to hidden trackers, either. As we at Yale Privacy Lab noted in November: "Many of the same companies distributing Google Play apps also distribute apps via Apple, and tracker companies openly advertise Software Development Kits compatible with multiple platforms. Thus, advertising trackers may be concurrently packaged for Android and iOS, as well as more obscure mobile platforms."

Transparency in software development and delivery leads to better security and privacy protection. Not only is auditable source code a requirement (thought not a guarantee) for security, but a clear and open process allows users to evaluate the trustworthiness of their software. Moreover, this clarity enables the security community to take a good, hard look at software and find any noxious or insecure components that may be hidden within.

The trackers we've found in Google Play are just one aspect of the problem, though they are shockingly pervasive. Google does screen apps during Google Play's app submission process, but researchers are regularly finding scary new malware and there are no barriers to publishing an app filled with trackers.

Finding a Replacement

Yale Privacy Lab is now collaborating with Exodus Privacy to detect and expose trackers with the help of the F-Droid app store. F-Droid is the best replacement for Google Play, because it only offers FOSS apps without tracking, has a strict auditing process, and may be installed on most Android devices without any hassles or restrictions. F-Droid doesn't offer the millions of apps available in Google Play, so some people will not want to use it exclusively.

It's true that Google does screen apps submitted to the Play store to filter out malware, but the process is still mostly automated and very quick— too quick to detect Android malware before it's published, as we've seen.

Installing F-Droid isn't a silver bullet, but it's the first step in protecting yourself from malware. With this small change, you'll

even have bragging rights with your friends with iPhones, who are limited to Apple's App Store unless they jailbreak their phones.

But why debate iPhone vs. Android, Apple vs. Google, anyway? Your privacy and security are massively more important than brand allegiance. Let's debate digital freedom and servitude, free and unfree, private and spied-upon.