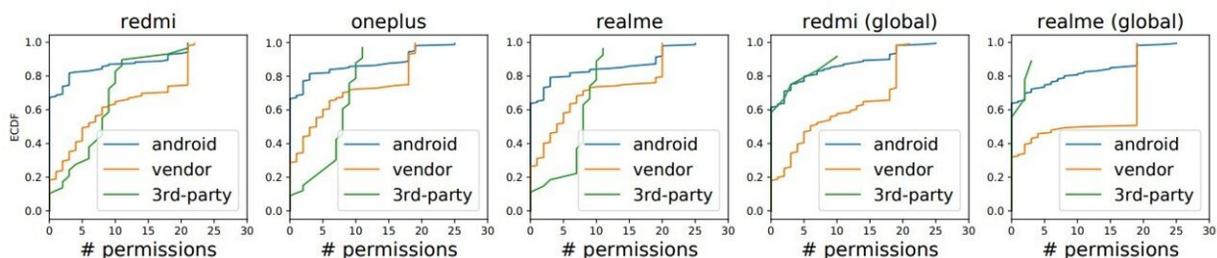


Android phones sold to customers in China found to be loaded with apps that send user data to third parties

February 9 2023, by Bob Yirka



The ECDF of the number of dangerous permissions requested by each category of packages in each handset. Credit: *arXiv* (2023). DOI: 10.48550/arxiv.2302.01890

A group of computer scientists, two from the University of Edinburgh, and a third from Trinity College, has found that phones purchased by customers in China are riddled with software that continuously sends user data to third parties without the permission or even knowledge of the phone's users. Haoyu Liu, Douglas Leith and Paul Patras have summarized their findings in a paper posted on the *arXiv* preprint server.

In the U.S. and many other countries, [phone users](#) take their privacy seriously—the maker of the phone, its operating system or installed apps are all expected to maintain a strict level of security. That security does

not appear to be the norm for vendors in China. In this new effort, the researchers purchased a number of phones in China and tested how well they protect private user information.

The testing involved phones made by companies such as OnePlus, Oppo Realme and Xiamoi, which are all popular in China. They tested not only the installed apps, but the underlying [operating system](#), a modified version of Android. Their overall goal was to determine the type and amount of personally identifiable information (PII) being sent from the phones to third parties.

The research team found that the phones were rife with applications sending [user data](#) to a variety of third parties, all without permission. During testing, they set phones to opt out of sending any sort of data to providers or any other third parties, and did not connect to cloud applications. Still, applications sent data to the makers of the phone, network operators and also to the makers of apps. Data included physical information such as the user's phone number, its MAC address and ongoing geolocation data. It also included more [personal data](#), such as contact lists and text metadata.

The researchers suggest that the phones sent enough information so that those on the receiving end would know who was using a phone, where it was and what the user was doing. They also found that there was no way to opt out of such privacy breaches and that the breaches continued even if the user took their [phone](#) outside of China.

More information: Haoyu Liu et al, Android OS Privacy Under the Loupe—A Tale from the East, *arXiv* (2023). [DOI: 10.48550/arxiv.2302.01890](#)

Citation: Android phones sold to customers in China found to be loaded with apps that send user data to third parties (2023, February 9) retrieved 4 May 2024 from <https://techxplore.com/news/2023-02-android-sold-customers-china-apps.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.