Google Inc.
1600 Amphitheatre Parkway
Mountain View CA 94043

650 253-0000 main
google.com

6 April 2020

Dear Mr. Hosein,

Thank you again for your Jan. 8 letter about pre-installed software on Android devices from third-party manufacturers. We appreciate the opportunity to engage with you on the work our Android privacy and security teams do to keep users safe across the Android ecosystem. I'm glad that we were able to connect your staff directly with our product experts on this issue, and as we've previously mentioned, we have shared your letter with a range of device makers and offered to put them directly in contact with Privacy International.

As promised, following some introductory comments about how Google approaches pre-installed apps on third-party Android devices, I've provided written responses below to the specific issues Privacy International raised. Our team welcomes the chance to continue the dialogue we've begun on these important issues.

Google agrees wholeheartedly that all Android users deserve the same high standard of protection from privacy abuses and security vulnerabilities. Because Android is an open ecosystem, transparency about our security work has been the hallmark of our approach. Our team speaks and writes frequently about its efforts across the ecosystem, including monthly security bulletins, annual reports, white papers, frequent blog posts, and presentations at public conferences attended by experts from throughout the security and privacy communities. We do this because sharing information with the Android ecosystem helps device makers and app developers improve their own practices, and because outside input, criticism, and other feedback helps us improve -- all benefiting consumers in the end.

Pre-installed software presents unique challenges -- and opportunities -- for Android. Android's flexibility allows device makers to customize their devices and compete more effectively through a differentiated user experience. As long as they meet compatibility requirements that ensure Android app functionality, device makers are free to include their own software on their devices, including software like app stores that competes directly with Google offerings such as Google Play. This variety makes Android special, and it's important to both device makers and consumers who choose their devices.

Of course, this flexibility necessitates greater vigilance in policing against potential security and privacy threats. Our teams have ramped up investment in this area over the last few years.

As one example, in 2018, we launched Build Test Suite (BTS) for partner device makers. Device makers submit their new or updated build images to BTS. BTS then runs a series of tests that look for security issues on the system image, including scanning for pre-installed potentially harmful applications (PHAs) included in the system image. If we find a PHA on the build, we work with the partner to remediate and remove the PHA from the build before it can be offered to users. During its first calendar year, BTS prevented 242 builds with PHAs from entering the ecosystem.

We also worked with Android device makers, mobile network operators, and system-on-chip vendors to increase the number of devices receiving regular security updates. Our combined efforts -- which include platform improvements, new agreements, and partner programs such as Android One and Android Enterprise Recommended -- increased the number of devices receiving security updates by 84%.

We frequently share examples of our work to raise the bar across the entire Android ecosystem, including this presentation about a problem we discovered with pre-installed apps, and how we forced device makers to remediate the issue, demanded post-mortems from them, and instituted new rules to prevent it from happening again. We shared this experience publicly at one of the most widely attended security conferences in the industry.

Although pre-installed software on third-party Android devices has sometimes presented privacy challenges, we do have concerns about the research cited by Privacy International from the IMDEA Networks Institute. When this research was first published, we noted questions about its accuracy and the broad conclusions it attempts to draw. Specifically, the majority of the phones tested were not Google compatible devices and did not have Google Play Protect, our built-in malware detection service. We asked the researchers to share samples of problematic apps with us, and none of the samples they shared to date turned out to be pre-installed apps.

Below are responses to the specific recommendations in your letter:

Individuals should be able to permanently uninstall the apps on their phones. This should include any related background services that continue to run even if the apps are disabled.

We agree that users should be able to choose which apps to run on their phones. All apps downloaded from Google Play can be uninstalled at any time. Additionally, users can disable most pre-installed apps that are not system critical by following the instructions available here.

As explained above, device makers ultimately decide which apps come pre-installed and there are sometimes good reasons to prevent users from deleting certain apps. For example, some basic functions of a mobile device are implemented as apps. These include phone dialers,

messaging clients, and camera apps. Other apps implement important services like mobile carrier services and data plan management. Allowing users to delete these apps risks compromising device functionality and, in some cases, may introduce new security or privacy vulnerabilities.

Pre-installed apps should adhere to the same scrutiny as Play Store apps, especially in relation to custom permissions.

We're proud of the security and privacy standards underlying Google Play, and we're continually raising the bar for apps on Google Play, both through Google Play Protect and our Google Play developer policies. We recently shared an overview of our work here.

Because Android users deserve a safe experience regardless of where their apps come from, we've been exploring ways to establish clearer baseline standards for pre-installed apps, analogous to our Google Play standard, while still respecting device makers' autonomy, the important role they have in protecting consumers, and the interest they have in creating the right experience for their customers.

For example, to align our policies for device makers with those for developers on Google Play, we require all pre-installed apps to use Android run-time device permissions. Device makers are permitted to pre-grant device permissions for certain pre-installed apps but those apps must clearly specify via an alternative user interface which device permissions they are using, as well as the app and app developer that is accessing data. The alternative user interface must also provide toggles for each requested permission. The only exception to these requirements is apps required for the core functionality of the device or to set up the device out of the box, as well as apps that address emergency scenarios. Additionally, we classify unwanted software, including apps that collect personal information without adequate notice or consent, as PHAs and we are regularly expanding our BTS system to detect such PHA behavior in pre-installed apps.

Even as we pursue new ideas on this front, Google Play Protect runs continuously on all Google compatible Android devices, scanning for potentially harmful applications regardless of whether they were installed from Google Play. If we discover vulnerabilities, we alert users and suggest that they remove or disable the app in question. We scan approximately 100 billion apps every day. Last year, Google Play Protect prevented more than 1.9 billion malware installs from non-Google Play sources.

Pre-installed apps should have some update mechanism, preferably through Google Play and without a user account. Google should refuse to certify a device on privacy grounds, where manufacturers or vendors have attempted to exploit users in this way.

Many device makers, mobile carriers, and developers of pre-installed apps do update their apps through Google Play, and you can find these apps easily by searching on Google Play.

Sometimes, device makers choose to use their own update mechanism for pre-installed software, either through their own app store or another mechanism. As I noted above, this flexibility is important in empowering device makers to provide their own unique user experience. Because we support an open ecosystem, we have not found it appropriate to require Android device makers to use Google Play exclusively, and have pursued other ways to raise the bar on security while respecting device makers' ability to innovate on their own terms.

Google Play requires a user account so that, among other reasons, we can efficiently provision app updates and help users manage their installed apps and any purchases they've made, whether paid apps or purchases within apps. User accounts also underpin other features we offer, such as parental controls and family sharing.

* * *

Thank you again for your feedback. We value Privacy International's leadership in advocating for high privacy standards, and I hope we will continue the fruitful dialogue we've begun with Privacy International about improving user security and privacy.

Very truly yours,

Kareem Ghanem
Senior Manager
Government Affairs & Public Policy
Platforms & Ecosystems