Annex 1

Research Methodology for Dynamic Analysis

We conducted a dynamic analysis of the apps, using Privacy International's testing environment, which consisted of the following components:

• A laptop running a Virtual Machine (using Oracle's VirtualBox) with mitmproxy in "transparent" mode (meaning that the connection is being intercepted without the knowledge of the client). Along with the necessary tools to create a functional network access point. The Virtual Machine is running Debian 10 (Buster)

• A Google Pixel Android Phone, Running Android 8.1 (Oreo) – we used Lineage OS, built from the Android Open Source Project (AOSP), in order to run later versions of Android on the device.

• A device (laptop) to run the Android Development Bridge (ADB) in order to install the mitmproxy certificate into the Systems Trust Store (as opposed to the Users Trust Store) due to security constraints introduced in Android 7.

All data being transmitted between third parties and apps is encrypted in transit using Transport Layer Security (TLS, formally SSL). Our analysis consisted of capturing and decrypting data in transit between our own device and third party servers (so called "man-in-the-middle") using the free and open source software tool called "mitmproxy", an interactive HTTPS proxy. Mitmproxy works by decrypting and encrypting packets on the fly by masquerading as a remote secure. In order to make this work, we added mitmproxy's public key to our device as a trusted authority. The data exists on our local network at time of decryption. We used the same Google Account we have used for our previous research on third party tracking in apps.

Once the research was completed and appropriate setting within the phone where selected (pertaining to Wi-Fi, certificate trust, security such as PIN and screen lockout and developer tools such as showing touches), the following steps were taken:

- Connect to a non-intercepting Wi-Fi
- Download all applications from the Google Play Store (location set to UK)
- Connect to mitmproxy VM (via Wi-Fi)
- Open the app, register (if required) and perform a number of normal activities within the app
- Save screenshots off the phone and stop the flow in mitmproxy
- Uninstall the app

LIMITATIONS

Many apps we analysed share data with Google or subsidiaries of Alphabet Inc., such as Crashlytics. All server communication is completed over SSL/TLS using packed-binary file formats, which means that we were unable to decipher which data is being shared, using the methodology we relied on in this research. Our findings section does not mention data shared with Google or subsidiaries of Alphabet Inc.