Journal of Research in Health Sciences
ISSN: 2228-7809 | https://jrhsjournal.com

Mobile Health Applications Accountability Framework for COVID-19

Dr. Emily Carter[1]*, Dr. James Liu[2], Dr. Sophia Martinez[1]
[1]Department of Internal Medicine, Johns Hopkins University School of Medicine, United States
[2]Division of Cardiology, Mayo Clinic, United States

Abstract

COVID-19 mobile applications (apps) play a critical role in combating the pandemic and treating those impacted by coronavirus. As governments, public health officials, and others rush to develop COVID-19 apps during the pandemic, it is important to ensure data protection and privacy are neither overlooked nor compromised. Over the last two months, the International Digital Accountability Council (IDAC) investigated 108 global COVID-19-related mobile apps spanning 41 countries to better understand the technology and privacy implications behind these apps. This investigation was prompted by the rapid development and deployment of COVID-19 apps in response to the COVID-19 pandemic.

Keywords – COVID-19; apps; privacy; security; investigation.

1 Background

Launched in April 2020, IDAC is led by an experienced team of lawyers, technologists, and privacy experts with a shared goal of improving digital accountability through investigation, education, and collaboration. As a nonprofit watchdog, IDAC investigates misconduct in the digital ecosystem and works with developers and platforms to remediate privacy risks and restore consumer trust.

IDAC believes COVID-19 apps were created with the best intentions under extreme time pressure. We appreciate the lengths to which many app developers have gone to incorporate privacy-by-design principles into their processes. This investigation is intended to help ensure that these important and widely used COVID-19 efforts can be successful by highlighting areas for improvement and offering actionable recommendations.

Our investigation did not reveal intentional or malicious misconduct. In many cases, we found that governments, developers, and their partners took great care to protect the privacy of users and adopted best practices in the design of the apps. However, our investigation did uncover several instances in which apps fell short of best practices related to privacy and security, and potentially exposed the public to avoidable risks and potential harms. In particular, we found that some apps: (1) were not transparent about their data collection and third-party sharing practices; (2) included third-party advertising and analytics software development kits (SDKs) that seemed extraneous to the functionality of the app; (3) sent transmissions that were not; and (4) requested permissions that have the potential to be invasive and may collect more information than is reasonably necessary to accomplish the core functions of the apps.

Our report concludes that, while most COVID-19 apps perform in ways that align with users' privacy expectations, there is clear room for improvement. In order to instill trust and encourage individuals to use these apps, developers must incorporate privacy by design principles, and carefully review their apps' permissions, third-party SDK integrations, and data transmission security. Our findings reveal privacy gaps that governments and companies creating these apps should address, especially in light of the need for public trust in order for COVID-19 management and mitigation efforts to succeed.

2 Methodology

Although new COVID-19 apps are being deployed frequently, IDAC investigated 108 COVID-19 Android apps that were available in the Google Play Store as of May 1, 2020. The investigation classified the 108 COVID-19 apps into four distinct categories: contact tracing, symptom checkers, telehealth, and quarantine administration. These apps were classified based on their main functions as well as their descriptions in the Google Play Store.

We conducted both static and dynamic analysis tests on these apps, as well as how they operated in real time. Using Android devices, we downloaded the apps and interacted with them in the way a typical user would. Next, we ran our analysis on the network traffic and additional operating system information that was generated while we were interacting with the apps. From these results, we were able to observe a variety of behaviors associated with the collection and transmission of personal information, including the types of personal data these apps collect, to

whom the data is being sent (looking with particular interest to transmission to third-parties), the types of permissions requested, the types of SDKs present in the apps, and other data transmissions.

3 Demographics

Our investigation included 108 Android apps spanning 41 countries. We found 58 apps that were developed by official government entities. 32 apps were developed by private organizations. Seven apps were created by a joint government and private entity effort, six by a health organization, and five apps were developed by a university.

4 Key Findings

The investigations found transparency, data protection, privacy, and security concerns, which are outlined further below. However, we did not identify any misconduct that we would characterize as egregious or evidently willful.

4.1 Transparency

In some instances, our investigation revealed a lack of transparency with regard to data collection and third-party sharing. Four apps did not provide users with a privacy policy at all, violating Google's developer policies. Some other privacy policies disclosed collection and third-party data sharing practices in a generic and vague manner. For example, numerous policies failed to specify which third-party companies received the data. In many cases, the policies lacked a clear commitment to anonymizing, aggregating, and deleting sensitive data once the pandemic passes.

Overall, the European apps we examined had particularly robust privacy policies, perhaps because they are subject to the General Data Protection Regulation (GDPR), a comprehensive privacy law that imposes specific disclosure requirements for entities that process the personal data.

Given the public discourse relating to contact tracing apps, we paid particular attention to how the apps' privacy policies and Google Play Store app descriptions disclosed information about the anonymization of user data. Of note, only 20 percent of the apps we examined explicitly mentioned anonymization of user data. The rest of the apps did not disclose whether they engaged in this practice in their app description or privacy policy.

4.2 Software Development Kits (SDKs)

In some cases, we found that third-party SDKs were present in apps. SDKs are packages of code and other assets that provide a specific functionality within an app. Due to the time and effort it saves, it is common for app developers to use third-party SDKs for the functionality that they provide.

It was not always clear whether these SDKs were actively enabling data to flow to third parties without the user's consent. It is possible that, in some cases, developers were simply using tools that, in a non-COVID-19 context, are acceptable, but here are not equipped to handle the sensitive information these apps collect. However, we believe that the presence of SDKs is sufficient to warrant further scrutiny because of the inherent data-sharing and collection practices that these SDKs could potentially provide. In eight COVID-19 apps, our investigation revealed the presence of third-party SDKs that related to analytics or advertising. In our view, analytics and advertising SDKs should not be present in COVID-19 apps because of the potential for these SDKs to collect personal information. Developers have a responsibility to understand how third-party SDKs function within their apps.

4.3 Security

We observed some apps sending unsecured transmissions (e.g., not using transport layer security (TLS)). This behavior is contrary to best practices, which require encryption of all communications from the device to the destination. This is especially critical when users have a higher expectation from official government apps. We observed six apps sending unencrypted transmissions. Notably, the CDC was observed sending unencrypted communications with a third-party to obtain assets and content. Although we could not determine the content of the transmissions, metadata about the user's activity can be correlated with the device metadata that we were able to observe (e.g., mobile carrier, operating system, device resolution, etc.).

Unencrypted transmissions allow the transmissions to be read by all parties from the device to the destination. If the transmission contains personal information, anyone along that chain can view the information and potentially misuse it. This behavior potentially exposes users' personal data to cyber-attacks and breaches. Given the sensitive nature of these apps, it is essential to follow recommended best practices for data transmissions.

4.4 Permissions

When users download a new app, the app asks for certain permissions to function. These permissions indicate the means by which an app is attempting to obtain data from a user's device -- either directly or by inference. Roughly half of the COVID-19 apps we tested request permissions that have the potential to be invasive if misused.

Although they are common, permissions such as "read external storage" or "write external storage" are nevertheless concerning because they can allow the app to access other shared files on the device that could be used to infer personal information about the user, such as location (through calendar invites or image metadata). We found 38 apps requesting permission to access location, two apps requesting the device's camera, and one app requesting access to the user's contacts, all of which Google classifies as "dangerous"[1] because these requests for permission provide access to sensitive data or functionality. To acquire these permissions, apps must explicitly ask users to grant them at the time the permission is first used. There may be legitimate justifications for these apps to collect dangerous permissions, but we remain concerned about the potential for abuse.

4.5 Third-Party Data Sharing

We observed apps sharing data with third parties, which we defined as any entity that is not a developer of the app. These apps are predominantly sending data to Google (e.g., gstatic) or Google-owned companies (e.g., Crashlytics).

4.5.1 ID Linking

Our investigations observed the restricted practice of ID linking by Branch.io in the privately-owned U.S.-based app, *How We Feel*. Here, we found the Android ID being sent simultaneously (and within the same transmission) with the Android Advertising ID (AAID).[2]

Google places restrictions on the practice of ID linking within mobile apps.[3] Linking identifiers creates a type of "supercookie" -- an identifier that is persistently associated with a device and cannot be easily removed. ID linking raises privacy concerns because of the ability to persistently track users' activities across apps. It is not readily apparent why this is occurring; however, collecting these identifiers together may bypass a device's privacy settings.

4.5.2 Android ID

We observed 11 apps collecting the Android ID, a persistent identifier. Of these 11 apps, seven sent the Android ID to their own servers, and four were observed sending it to a third-party. Those third-parties include Branch.io, Bugfender, and Appcelerator.

4.5.3 Android Advertising ID (AAID)

We observed five apps collecting the AAID, and four of them were sending it to a third-party. This finding stood out to us because the AAID is used for advertising purposes, which we do not expect in COVID-19 apps. The third-parties receiving users' AAID include Facebook, Crashlytics, Branch.io, and OneSignal.

5 IDAC Recommendations

The COVID-19 apps we studied varied considerably in their implementation and approach to protecting users' privacy. Some apps were more effective than others at including privacy-preserving features. In order to instill trust and encourage individuals to use these apps, privacy must be a priority. We encourage app developers to put privacy concerns at the forefront of their development efforts. In particular, we recommend that developers ensure that all communications are encrypted, that permissions requested be narrowly tailored, and that developers refrain from including unnecessary third-party SDKs. Additionally, developers must be transparent and clear about how users' data is collected, used, retained, stored, and shared.

Although our technical findings did not identify any specific evidence of data misuse in connection with quarantine apps administered by governments, these efforts pose potential concerns about how data collected from those apps will be used and retained, particularly by governments with poor human rights records.

---

1 https://developer.android.com/guide/topics/permissions/overview

2 The Android Advertising Identifier (AAID) is an identifier created by Google for the purpose of ad tracking that still allows the user to have some control since they users can reset their AAID from the settings on their device. The use of AAID is a best practice for apps that use ad monetization. However, in the case of COVID-19 apps, serving ads on apps that handle such sensitive information may be a privacy concern, and should not allow any SDKs to track user information for advertisement and marketing purposes.

3 https://developer.android.com/training/articles/user-data-ids

Developing technological tools rapidly to aid in public health efforts to combat a worldwide pandemic is an inherently difficult task. Under the circumstances, our investigation revealed that many COVID-19 app developers and their government partners took responsible steps to protect users' privacy and the security of sensitive data. We applaud their efforts and we offer the suggestions in this report in the spirit of constructive feedback meant to improve the efficacy of a critical effort. By taking these additional steps, as well as other precautionary measures, developers can assure that user data is handled responsibly, and inspire the trust necessary to facilitate public participation in critical pandemic response efforts.

6 Updates Post-Report

A few notables updates have occurred since the release of our original report on June 5, 2020. Our team has since briefed developers, government officials, and journalists on our investigatory findings, with the goal of raising the bar for privacy and security for COVID-19 apps. The following are updates to some apps that our report covered.

Kinsa for Wireless Smart Thermometers: according to the Washington Post, who published an article citing our report on June 22, Kinsa's app will no longer send the Android ID, a persistent unique identifier, to Branch.io, a third-party analytics and mobile growth company. Kinsa informed the Washington Post they were "previously unaware that Branch was receiving data that could be used for targeted advertising and disallowed access for Android phones last week following IDAC's report."[4]

COVID-19 Tracker by Medinin: this Indian contact tracing app is no longer available to download in the Google Play Store. We identified major areas of concern with regards to this app, including that it (1) copied another app's privacy policy, (2) sent unencrypted transmissions to an API and obtained users' COVID-19 symptom reports and location data, and (3) collected the device IMEI, a non-resettable unique identifier that should have not been collected. The public API that contained users' data is also no longer available either. These findings raised serious privacy and security concerns for our team and we are pleased that the app is no longer available for users to download.

patientMpower for COVID-19: IDAC had the opportunity to speak with patientMpower and learned that we miscategorized their apps as symptom checkers, when they are a telehealth apps. Users are unable to download the app unless they are enrolled by their healthcare provider. We learned that although patientMpower notified the Irish Data Protection Commissioner of their use of Urbanairship's SDK, they plan to retire its use. Further, patientMpower clarified that their apps use analytics SDKs for the necessary purposes of monitoring patient blood oxygen levels and sending push notifications to alert patients when there are changes to their blood oxygen levels.

Smittestopp: on June 15, the Norwegian Institute of Public Health Following suspended Norway's contact tracing app, *Smittestopp*, for concerns around collection geolocation data and it's use of the centralized app architecture.[5] The app, however, is still available to download in the Google Play Store.

Bolivia Segura: at the time of the report's release, this app did not have a privacy policy posted in the Google Play Store, in violation of Google's Developer Policies. We notified them and they have since posted a privacy policy.

NICD COVID-19 Case Investigation: our report drew attention to this app's lack of a privacy policy. The app is no longer is available to download in the Google Play Store.

Cova Punjab: we flagged the Indian-owned *Cova Punjab* app for its collection of persistent identifiers such as the IMEI and service set identifiers (SSID), which could be used to track users over time. At the time of our report's release this app was in the process of being retired and it is currently no longer available in the Google Play Store. However, a newer version of this app, *COVA Punjab*, is available to download and our team did not observe this newer app collecting persistent identifiers.

Acknowledgements

IDAC would like to thank our partners at Good Research, AppCensus, The Future of Privacy Forum, and The German

4 https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/22/the-cybersecurity-202-privacy-experts-say-many-coronavirus-apps-aren-t-doing-enough-to-safeguard-users-information/5eefae20602ff12947e91075/

5 https://techcrunch.com/2020/06/15/norway-pulls-its-coronavirus-contacts-tracing-app-after-privacy-watchdogs-warning/

Marshall Fund of the United States for their support and assistance with this report.