IDAC
International Digital
Accountability Council

COVID-19 Mobile App Accountability Investigation Recommendations

Quentin Palfrey[1], Lena Ghamrawi[1], Nathan Good[2], Will Monge[2],
**qpalfrey@digitalwatchdog.org*

[1]International Digital Accountability Council, United States
[2]Good Research, United States

Abstract

COVID-19 mobile applications (apps) play a critical role in combating the pandemic and treating those impacted by coronavirus. Developing technological tools rapidly to aid in public health efforts to combat a worldwide pandemic is an inherently difficult task. 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. From May - June 2020, 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. While the COVID-19 app landscape has changed since June, the recommendations that arose in connection with the investigation remain helpful for developers and governments that are currently deploying COVID-19 apps.

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.

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 order to instill trust and encourage individuals to use these apps, developers must incorporate privacy by design principles. 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. Our goal is to use our investigatory findings and offer actionable recommendations.

Recommendations

1. **Transparency**

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 vague manner. We recommend that all apps should provide a clear privacy policy that explains how user data will be collected, shared, used, and retained.

2. **Software Development Kits (SDKs)**

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 over collect personal information. Developers have a responsibility to understand how third-party SDKs function within their apps and should only use SDKs that are necessary for the app to provide its functionality.

3. **Unsecured Transmissions**

We observed six apps sending unsecured transmissions (e.g., not using transport layer security (TLS)), which poses cybersecurity risks. This behavior is contrary to best practices, and we recommend apps to encrypt all communications from the device to the destination.

4. **Permissions**

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" because these requests for permission provide access to sensitive data or functionality. We recommend that apps only require permissions that are needed for the app to function, and to explicitly ask users to grant them permission at the time the permission is first used.

By taking these additional steps, as well as other precautionary measures, developers and governments can help ensure that user data is handled responsibly, and inspire the trust necessary to facilitate public participation in critical pandemic response efforts.