Privacy in the Age of COVID:
An IDAC Investigation of COVID-19 Apps

June 5, 2020

COVID-19 mobile 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 spanning 41 countries to better understand the technology and privacy implications behind these apps.[1] This investigation was prompted by the rapid development and deployment of COVID-19 apps in response to the COVID-19 pandemic.

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 and we take into account the time-sensitive and hurried conditions under which they were developed. 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 encrypted -- including the U.S. Centers for Disease Control and Prevention (CDC) app; 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.

[1] IDAC would like to thank our partners at the Future of Privacy Forum, Good Research, AppCensus, and the German Marshall Fund of the United States for their support and assistance with this report.

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,[2] 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.

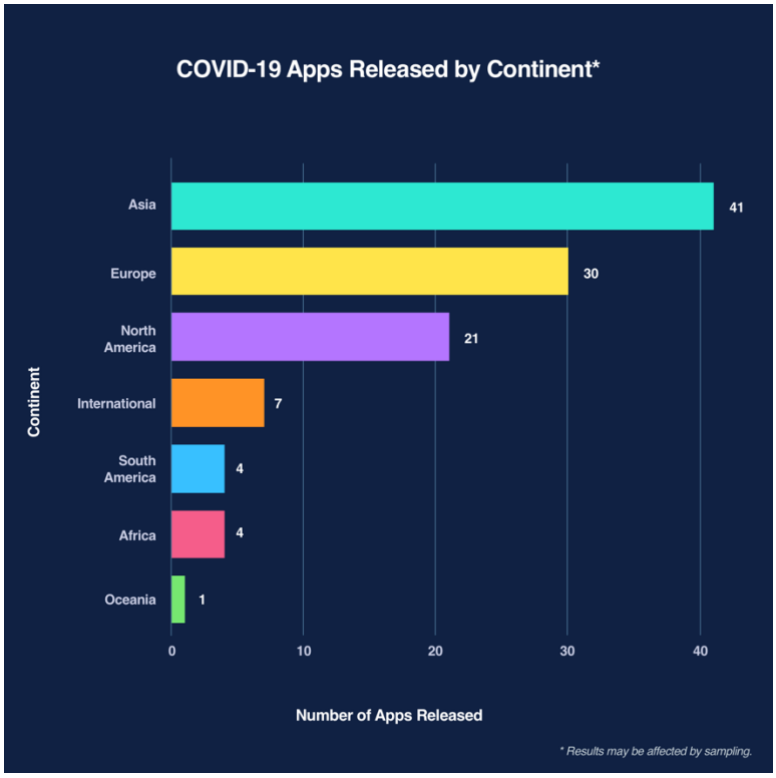
Methodology

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 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.

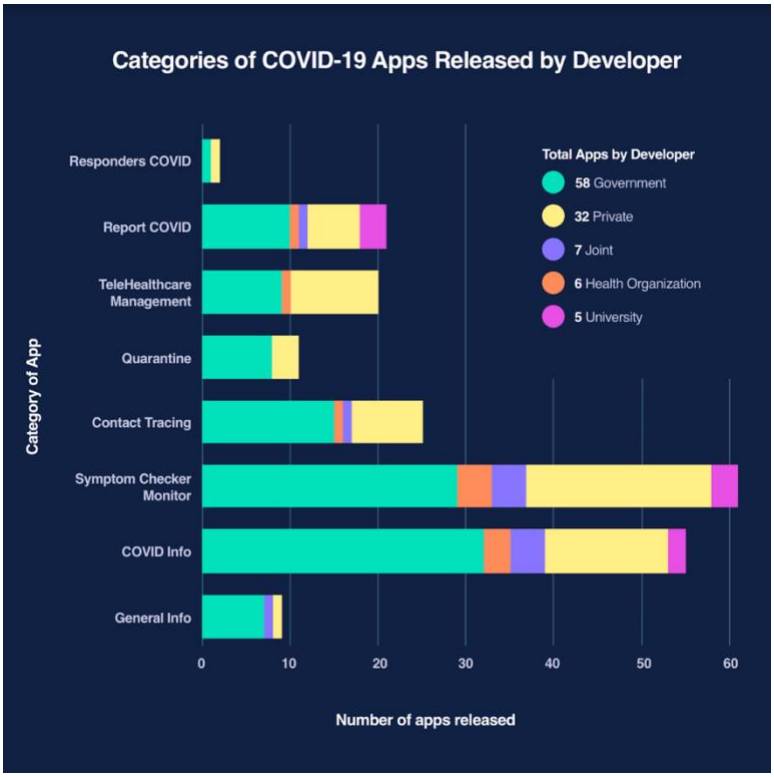
Demographics

Our investigation included 108 Android apps spanning 41 countries. The distribution illustrates that countries in Asia have developed the most COVID-19 apps, with India developing more apps than any other country (18 apps). Europe is the next, with 30 apps that we tested. These reflect the higher number of incidents of infection in these areas, and it is possible that other continents may soon follow suit.



We found that 58 apps have been developed by official government entities, which highlights the fact that governments are using technology to combat the pandemic in unprecedented ways. 32 apps were developed by private organizations, although it appears that some of these companies work closely with governments or local public entities based on apps they have previously published. 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.

[2] For example, as established by the Information and Privacy Commissioner of Ontario privacy by design framework.



Key Findings

The investigations found some 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.

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.

Software Development Kits (SDKs)

In some cases, we found that third-party SDKs were present in apps. 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. Developers have a responsibility to understand how third-party SDKs function within their apps.

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. 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.

Permissions

Many apps in our investigation request permissions that have the potential to be invasive. 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 also found apps requesting location or camera permissions, which Google classifies as dangerous. There may be legitimate justifications for these apps to collect dangerous permissions, but we remain concerned about the potential for abuse.

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.

Please continue reading the full investigative report below.

Table of Contents

I. Key Findings

A. Transparency

Our investigation revealed a lack of transparency with regard to data collection and third-party sharing. In many cases, the privacy policies lacked a clear commitment to anonymizing, aggregating, and deleting sensitive data once the pandemic passes. At a first glance, we observed four apps that did not provide users with a privacy policy at all, in apparent violation of Google's Developer Policies.[3]

The following apps did not have a privacy policy linked in the Google Play Store:

- NICD COVID-19 Case Investigation (South Africa/Gov)
- Kenya Covid-19 Tracker (Kenya/Private)
- Bolivia Segura (Bolivia/Gov)
- COVID-19 Tam (Mexico/Gov)

Additionally, the disclosures provided by the privacy policies that were linked in the Google Play Store varied widely. Some privacy policies were detailed and tailored to the app's personal data and privacy practices. Other policies fell far short of best practices.

Some privacy policies we examined disclosed collection and third-party data sharing practices in a generic and vague manner, making it appear that they used template language borrowed from other privacy policies. For instance, the government-owned Indian app *Corona Watch*[4] and privately-owned Indian app *COVID-19 Tracker by Medinin*[5] have virtually the same templated privacy policy. Neither policy explicitly references COVID-19 and neither discloses the purpose of data collection beyond vague statements such as, "the personal information that we collect is used for providing and improving the Service."

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.

Specifically, when analyzing contact tracing apps, we compared seven European and five Indian apps' privacy policies. On average, European apps' privacy policies were twice as long (2,100 English words[6] vs. 1,000 English words) and were more likely to:

- Describe how data is collected;
- Mention and provide the name and contact information of a privacy officer;
- Describe data retention practices; and
- Describe the privacy rights users have in relation to their personal data.

[3] https://play.google.com/about/privacy-security-deception/user-data/#!?zippy_activeEl=personal-sensitive#personal-sensitive

[4] http://kgis.ksrsac.in/privacystatement/

[5] https://www.medinin.com/privacy-policy

[6] Five European privacy policies were translated to English using Google Translate. All Indian privacy policies were already in English.

Only one of the five Indian apps we analyzed provided these basic privacy disclosures, whereas six of the seven European ones did.

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.

B. Software Development Kits (SDKs)

In eight COVID-19 apps, our investigation revealed the presence of third-party SDKs that related to analytics or advertising. 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.

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. The presence of these SDKs does not necessarily imply that the SDK is actively transmitting user data to third parties. Nevertheless, the use of these mixed-purpose SDKs presents a challenge and additional burden on the developer to ensure that the ad and analytics components are not being used or are disabled to prevent the inadvertent transmission of personal data to third parties.

Many developers are familiar with using these types of SDKs as a matter of course. However, in the COVID-19 context, they may have unintended side effects that could potentially compromise other carefully constructed privacy measures in the app in ways that a developer did not anticipate. SDKs that would be appropriate in a non-pandemic context were not designed to accommodate the sensitive nature of a COVID-19 app. Consequently, there is a potential for extraneous sensitive information to be sent out in conjunction with the use of these apps. This is particularly true in the case of SDKs that provide monetization capabilities.

It is important to note that our tests did not reveal active personal data transmissions in connection with the SDKs that were present in the apps we analyzed. In some cases, developers may have legitimate reasons to include these SDKs that are tied to intrinsic functionality for the app. It is also possible that developers who were quickly writing apps simply used these SDKs for some functionality unrelated to ads or analytics, or that they were added by default in association with other tools.

Below are the apps we tested that had a concerning SDK present.

App Name	Country/Developer	App Category	SDK (category) Present in App
Kencor COVID-19	USA/Private	Symptom Checker, Telehealth	Google Ads (advertising) and Crashlytics (analytics)
patientMpower for COVID-19	Ireland/Private	Symptom Checker	Urbanairship (analytics)
patientMpower for COVID-19 USA	USA/Private	Symptom Checker	Urbanairship (analytics)

BC COVID-19 Support	Canada/ Gov + Private	Symptom Checker	Crashlytics (analytics)
Kinsa for Wireless Smart Thermometers	International/ Private	Symptom Checker, Telehealth	Crashlytics (analytics)
Canada COVID-19	Canada/Gov	Symptom Checker	Crashlytics (analytics)
TraceTogether	Singapore/Gov	Contact Tracing	Crashlytics (analytics)
T COVID'19	India/Gov	Symptom Checker, Telehealth	Umeng (social network)

We encourage developers, even those trying to do their best under rushed conditions, to closely review the types of third-party SDKs they place in their apps and only use what is absolutely needed for the core functionality of the apps.

C. Security

Given the sensitive nature of these apps, it is essential for developers to follow recommended security protocols for data transmissions. This is especially critical when users have a higher expectation from official government apps. We observed six apps sending unsecured transmissions. For example, these apps did not use cryptographic protocols designed to provide communications security over computer networks such as transport layer security (TLS). Best practices in the development of apps -- particularly COVID-19 apps that relate to sensitive information -- require encryption of all communications from the device to the destination.

All the transmissions that were observed sending data unsecured were sent to a server owned by the app or sent to third parties for the purposes of obtaining ads, images, or other assets. We found two apps sending personal or sensitive data unsecured.

The dangers of exposing data through unencrypted transmissions are profound. If transmissions are not secured, they can be read by all parties along the chain from the device to the destination. If personal data is sent unsecurely, it becomes exposed to an array of cyber-attacks, breaches, and other potential misuse.

Two apps were found sending unsecured transmissions that could be potentially harmful for users due to the sensitive nature of the data transmitted:

- **COVID-19 Tracker by Medinin (India/Private)** sends the device IMEI,[7] precise global positioning system (GPS) coordinates,[8] physical home address (in some instances), and the user's reported COVID-19 symptoms.

7 The International Mobile Equipment Identity (IMEI) is a unique identifier of the physical device that cannot be changed. It is prohibited to change the IMEI in some jurisdictions, including the United Kingdom. It does not change with factory resets and therefore remains the same even for refurbished mobile devices.

8 The data had GPS coordinates with seven decimals, which is precise up to inches (*source*: http://wiki.gis.com/wiki/index.php/Decimal_degrees). When we cross-referenced the GPS coordinates with some of the addresses, we were able to match to within a few feet.

- **COVID-19 Gov PK (Pakistan/Gov)** sends the COVID-19 symptoms, preconditions, fever status, and other information reported by the user in order to obtain the assessment result. No personal data was observed in these transmissions, but transmissions metadata could be used to infer location, including home address.

We observed two other apps sending unsecured transmissions worth mentioning, although the risks for users are lessened because we did not observe personal data in these transmissions.

- **news.gov.hk 香港政府新聞網 (Hong Kong/Private)** transmits information unsecurely and we were able to observe the articles being accessed and read by the user, as well as other in-app user activity. Additionally, this app communicates to a third-party[9] to obtain ads. However, the transmissions do not indicate that the ads were targeted or that the app was sending any personal information or identifiers.

- **Centers for Disease Control and Prevention (USA/Gov)** communicates unsecurely 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.).

```
--------------------------------
(packet) gov.cdc.general outbound to cdc.sc.omtrdc.net:80 (54.218.180.161) not encrypted at time 1588197561248
--------------------------------
POST /b/ss/cdcsynd/0/JAVA-4.17.0-AN/s82528494 HTTP/1.1
connection: close
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Linux; U; Android 9; en-US; AOSP on sargo Build/PD2A.190115.032)
Accept-Language: en-US
Content-Length: 640
Host: cdc.sc.omtrdc.net
Accept-Encoding: gzip

ndh=1&ce=UTF-8&c.&a.&CarrierName=Mint&AppID=CDC 2.7.1 (271000005)&RunMode=Application&OSVersion=Android
9&TimeSinceLaunch=231&Resolution=1080x2088&DeviceName=AOSP on sargo&.a&channel=OADC&gov.&cdc.&appframework=CDC Mobile Hybrid
Framework&partnerdomains=http://www.cdc.gov/outbreaks/&appname=CDC&contentsourceurl=modal-menu-open-navigation&language=en-
US&appversion=2.7.1.5&osversion=9&devicetype=handset&eventname=Open Modal:
Menu&osname=Android&sectionname=Outbreaks&status=1&.cdc&.gov&.c&t=00/00/0000 00:00:00 0
420&pageName=Navigation&aid=[redacted]&cp=foreground
```

Centers for Disease Control and Prevention app packet showing unencrypted transfer

The privately-owned Indian *COVID-19 Tracker by Medinin* app poses additional security concerns. The app communicates unsecurely to an application programming interface (API) and obtains a full list of users' COVID-19 symptom reports. This API is unsecure, meaning it can be queried by anyone that has the hostname. Our tests revealed that a simple query to the API sends back a list of reports that include highly accurate GPS, physical address (in some cases), the symptoms reported by the users, and the time of the report. This is concerning, as this information could potentially be combined to re-identify individuals.

Below is the list of apps we observed sending unsecured transmissions.

[9] The domain is registered under a different company by the name of Network Solutions, LLC (*source*: information obtained from ICANN on June 3, 2020: https://lookup.icann.org/)

App Name	Country/Developer	App Category	Transmission Data
COVID-19 Tracker by Medinin	India/Private	Contact Tracing, Symptom Checker	Geolocation, address, IMEI, user-reported symptoms
COVID-19 Gov PK	Pakistan/Gov	Symptom Checker	Symptoms, preconditions, assessment result, aggregate COVID-19 statistics
news.gov.hk 香港政府新聞網	Hong Kong/Gov	General Information	Device data, articles accessed by the used (full content) and advertisements
Centers for Disease Control and Prevention	USA/Gov	Symptom Checker	Device information (e.g., mobile carrier, operating system, device resolution) and activity metadata
COVID-19 Tam	Mexico/Gov	Symptom Checker	Aggregate county level statistics from an unsecure API
Alertes info: Actualité locale et alerte d'urgence	France/Private	General Information	Images, other assets, and client heartbeats to the server (online status)

D. 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 common, permissions such as "read external storage" or "write external storage" can allow apps 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"[10]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. For example, the privately-owned U.S.-based app, *Healthy Together COVID-19*, requests to "read contacts." The app apparently uses this permission to enable users to share information with friends more easily. However, the consequence of this permission is that the app has access to all of the users' contacts, which the users may not want the app to have. The core functionality in this case is sharing with particular individuals, but the permission gives access to all contacts.

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

E. 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).[11] The table below demonstrates the information Google, Crashlytics, and other third parties collect.

App Name	Country/ Developer	App Category	Data Sent to Third Parties	Third Parties Receiving Data	Third-Party Data Sharing Practices Disclosed in Privacy Policy?
Private Kit	USA/ Private	Contact Tracing	Assets, data from health authorities with location + random string identifier, and binary data	Gstatic.com, google.com, githubusercontent .com	Yes
TraceTogether	Singapore/ Gov	Contact Tracing	App build information	Googleapis.com, crashlytics.com	Yes
eRouška - Part of Smart Quarantine	Czech Republic/ Gov	Contact Tracing	App build information, with some non-identifiable aggregate information: time zone, country, language, operating system version, etc.	Googleapis.com, crashlytics.com	Yes
StopKorona!	Poland/ Gov	Contact Tracing	App build information	Google.com, gov.mk, googleapis.com, crashlytics.com	Yes
Hamagen (The Shield - The National App for Coronavirus War)	Israel/Gov	Contact Tracing	App build information	Googleapis.com	Yes

[11] Other studies have reported that the privately-owned North and South Dakota app (Care19) shares data with Foursquare. https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/ If indeed Care19 shares data with a commercial entity, this data-sharing raises privacy concerns even if the purpose of this data sharing is to alert local businesses about the spread of the virus. Care19 cannot be sure that these third parties will engage in adequate privacy and security controls once user data is transmitted to them. Moreover, users do not expect their personal information to be shared with commercial entities and it may be difficult for users to hold Foursquare accountable to honor Care19's commitments with regard to how it uses their personal data.

Aarogya Setu	India/ Joint Gov and Private	Contact Tracing	App build information, with some non-identifiable aggregate information: time zone, country, language, operating system version, etc.	googleapis.com, crashlytics.com	No (privacy policy not accessible)
Care19	USA/ Private	Contact Tracing	Android ID to bugfender. App build information to google (Firebase) and Crashlytics	bugfender.com, googleapis.com, crashlytics.com	Yes
Corona Tracking and Response App	India/Gov	Contact Tracing	App build information	crashlytics.com	Yes, but in vague terms
Healthy Together- CV 9	USA/ Private	Contact Tracing	App build information, with some non-identifiable aggregate information: timezone, country, language, operating system version, etc.	Google.com, googleapis.com, gstatic.com, crashlytics.com	Yes
COVID-19 Tracker by Medinin	India/ Private	Contact Tracing	App build information	google.com, gstatic.com	Yes, but in vague terms
Corona 360	France/ Private	Contact Tracing	App build information	Gstatic.com, google.com, crashlytics.com	Yes, but in vague terms
98point6	USA/ Private	Telehealth	Device to Auth0.com. Build information to launchdarkly.com	Auth0.com,[12] launchdarkly.com	Yes
Kinsa for Wireless Smart Thermometers	International/Private	Telehealth	Android ID to branch.io. Build information to crashlytics	Branch.io, ctfassets.net, crashlytics.com	Yes
Kencor COVID-19	USA/ Private	Telehealth	AAID and build information to crashlytics	Google.com, crashlytics.com	No
Tawakkalna (Covid-19 KSA)	Saudi Arabia/	Quarantine Admin	Build information	Googleapis.com, crashlytics.com	No

[12] Auth0 is a platform that handles secure authentication. The presence of Auth0 in our findings does not concern us.

	Gov				
CG Covid-19 ePass	India/ Private	Quarantine Admin	App build information, with some non-identifiable aggregate information: time zone, country, language, operating system version, etc.	Googleapis.com, firebaseio.com, crashlytics.com	Yes
COVID-19 West Bengal Government	India/ Gov	Quarantine Admin	Build information	crashlytics.com	No
TN COVID -19 TELE CONSULTATION	India/ Private	Quarantine Admin	Build information	Googleapis.com, crashlytics.com	No
TN HQ VC –NHM – DOCTORS APP COVID-19 S.0.S.	India/ Private	Quarantine Admin	Build information	Googleapis.com, crashlytics.com	No

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*. We found the Android ID being sent simultaneously (and within the same transmission) with the Android Advertising ID (AAID).[13]

Google places restrictions on the practice of ID linking within mobile apps.[14] 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.

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. One app that concerned us was the U.S.-based privately owned *Kinsa for Wireless Smart Thermometers* because this app appears to be marketed for families with young children. We observed them sending the Android ID to Branch.io, a third-party mobile growth and analytics company.

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.

13 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.

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

II. Category-Specific Findings

A. Contact Tracing Apps

Unlike other types of COVID-19 apps that serve multiple purposes, contact tracing apps are a distinct category of their own, as they have been created specifically to track the spread of the coronavirus. Contact tracing is a disease control measure that public health officials deploy to help determine the spread of the virus, as well as to prevent further spread. Contact tracing apps work by using location or proximity to identify and notify those that have been exposed to an infected individual. Location refers to the geographic location of the user. Proximity refers to the relationship between where the user is and where other users are, for example an individual who has been infected with COVID-19, or an individual with whom the app user has had close contact during a period of time when the user was contagious with COVID-19.

Investigation Limitations
Although our team was able to detect and analyze 23 contact tracing Android apps, we were only able to test 16 apps thoroughly due to the strict verification controls these apps have in place. The full list of these apps can be found in **Appendix A**.

App developers and origins

Our team analyzed 23 contact tracing apps from 16 countries, including a 11 from Asia, three from North America, seven from Europe, and two from Africa.

13 of the 23 contact tracing apps we tested were developed by government entities. Eight apps originated from private/commercial developers. One app was created through a joint private and government partnership. One app was created by a health organization.

Personal data collection

One of the general trends we noticed during our examination is that these apps are not collecting more personal data than is necessary from users. We observed four apps collecting geolocation data, which was disclosed in the app's privacy policy or the app's Google Play Store description.

One app collected the device hardware identifier, which raises privacy concerns around long-term user tracking. The privately-owned Indian *COVID-19 Tracker by Medinin* app was observed collecting the device IMEI, which is a non-resettable unique identifier. The practice of collecting hardware identifiers goes against widely recognized best practices because it is nearly impossible for users to reset these identifiers. As a result, there is the risk that users may be tracked across different apps, services, and devices. Moreover, it is challenging to determine a legitimate reason for this contact tracing app to collect the device's hardware identifier.

The use of GPS, Bluetooth, and manual logging for contact tracing

There are multiple ways that contact tracing apps function. We labeled five apps as "manual logging" apps. These apps enhance manual contact tracing efforts by assisting users in documenting where they were on a particular day, as well as with whom they came into contact.

Five apps use GPS or other methods to determine where a user had traveled. In some cases, it was not clear if users input their location into the app or whether the app automatically collects that data.

Lastly, we found six apps that use Bluetooth to detect proximity. Bluetooth allows a user's device to communicate with other devices nearby. While Bluetooth provides greater precision than geolocation, it also comes with privacy and security risks that must be managed.

Restrictions on self-reporting positive cases

Half of the contact tracing apps we tested prohibit users from self-reporting positive cases without verification from a credible healthcare provider. The remaining apps allow users to self-report without verification of a medical diagnosis.

Privacy-preserving features

A few apps incorporate privacy-preserving features to allow users more control over their personal data. For example, we observed at least two apps that do not allow data to leave the device, meaning that users' data is not sent to an external server, a recognized best practice. Below are examples of practices we advise other developers to consider emulating.

- **Care19 (USA/Private)** allows users to delete data in-app and excludes home location data (it uses the radius of where users have traveled instead of exact location points).

- **Smittestopp (Norway/Gov)** is explicit about deletion and allows users to delete their data in-app. The app informs users about maintaining the anonymity of those who have tested positive, but acknowledges its limitations.

- **TraceTogether (Singapore/Gov)** encrypts data, has simple and clear in-app terms, and informs users that the app will no longer be available after the pandemic subsides.

- **COVID Safe Paths (USA/Private)** requires users to provide consent before any data leaves the device. Additionally, no personal data is shared and the app allows users to turn their location off in the app.

- **Corona 360 (France/Private)** shows a map of positive case reports and allows users to check the map and infer tracing on their own. To protect the privacy of others, the app does not allow users to pinpoint exact addresses on the map.

- **StopKorona! (Poland/Gov)** encrypts all data and exchanges a randomly generated code with other devices in order to protect the identity of users.[15]

- **Corona Watch (India/Gov)** does not do individual contact tracing but provides a map of positive cases so users can conduct their own contact tracing.

[15] Although this is much better than exchanging an identifier that could be tied back to the device or the user, this identifier remains fixed over time. That means this approach is vulnerable to attackers gaining knowledge of the movement of individuals. Other approaches (such as the Google/Apple Exposure Notification framework) change these codes so as to protect against eavesdroppers tracking the movements of individuals.

B. Symptom Checker Apps

Symptom checker apps are used by individuals to determine if they may have COVID-19. Individuals record their personal information and any symptoms they may be experiencing in order to obtain a preliminary diagnosis or more information about what next steps and treatment options are available.

Investigation limitations
Although our team was able to detect and analyze 60 symptom checker Android apps, we were only able to thoroughly test 44 apps due to installation restrictions. Even with the 44 apps, we faced some obstacles. For example, some apps required an account or specific information to be used. In those instances, we were not able to test the full range of functionality of each app. The full list of these apps can be found in **Appendix B**.

App developers and origins

The 60 symptom checking apps came from 28 countries. The apps we tested included 22 from Asia, 16 from North America, 13 from Europe, four from South America, three from Africa, and two that are worldwide, including an app developed by the World Health Organization.

We observed that half of the symptom checking apps were developed by government entities, while private developers created 21 apps. The rest of the apps were created either by a health organization or a university.

In addition to providing symptom assessments, 16 of the 60 apps also reported other COVID-19-related statistics such as infection rates or hotspots, with varying levels of granularity. For example, some apps reported statistics at a regional level while others reported by province or state.

Personal data collection

Our team observed symptom checker apps collecting the following types of personally identifiable data: phone number, email address, geolocation, and the AAID. With the exception of the AAID, which we typically expect to find in apps that serve advertisements, the collection of the other information is not unexpected.

Two India-based apps -- privately-owned *COVID-19 Tracker by Medinin* and the government-owned *Cova Punjab* app -- collect persistent identifiers such as the IMEI and service set identifiers (SSID).[16] The collection of IMEI and/or SSID raises privacy concerns because the IMEI and SSID are persistent identifiers, which means they are effectively tied to the device's hardware and are almost impossible to reset. It is difficult to find a legitimate reason for these two apps to collect the device's persistent identifiers in order to provide a COVID-19 symptom assessment.

Immediate vs. long-term symptom assessment

Individuals who use immediate symptom checking apps input their current symptoms and get an immediate assessment. About 30 percent of these apps ask individuals to return to the app again over the next few days and input their symptoms, which we classify as long-term symptom assessments.

[16] The Service Set Identifier (SSID) is the name of the WiFi router that the device is either connected to or can perceive in the vicinity. The SSID is the human friendly WiFi name, which is not guaranteed to be globally unique, although many routers have unique default SSIDs. The SSID does not uniquely identify a user, as it may change throughout the day and the router may have more than one user. It does, however, give coarse-grained location data of a comparable accuracy to GPS.

Privacy-preserving features

Only a handful of the apps we tested disclosed whether they anonymized or encrypted user data. The following apps disclose whether they encrypt, anonymize, or aggregate user data:

Encryption[17]

- NCOVI (Vietnam/Gov)
- BC COVID-19 Support (Canada/Gov + Private)
- Canada COVID 19 (Canada/Gov)
- COVI (Qatar/Private)
- Healthy Together - COVID-19 (USA/Private)

Anonymization[18]

- Kinsa for Wireless Smart Thermometers (International/Private)
- COVID Radar (Netherlands/Health Organization)

Aggregation[19]

- HowWeFeel: The How We Feel Project (USA/Private)
- Canada COVID 19 (Canada/Gov)

[17] Encryption refers to the process by which information is transformed into a scrambled text that should only be understood by certain authorized parties.

[18] Anonymization is generally understood as a data sanitation process that focuses on preserving the privacy of the individuals within the data. Two common ways of anonymizing data are: removing specific personally identifiable information or encrypting the entire (or the "risky" parts of a) dataset.

[19] Aggregation is the process of combining information from multiple people together (grouped by common traits) so as to be able to obtain some general information while trying to reduce as much as the potential disclosure of information about particular individuals.

C. Telehealth Apps

Telehealth apps are used by individuals who are seeking COVID-19 healthcare treatment or services via their mobile device. On the whole, our investigation found that these telehealth apps generally exhibited good privacy and security practices.

Investigation limitations
Although our team was able to detect and analyze 20 COVID-19 telehealth Android apps, we were not able to access all of these apps because some required a government-issued identification or a local phone number to login. Some apps we tested were not specifically created for COVID-19 but were existing government-owned apps. The full list of these apps can be found in **Appendix C**.

App developers and origins

Our team was able to analyze 20 telehealth apps from ten countries: nine from Asia, four from North America, six from Europe, and one available internationally.

We observed that nine of these apps were developed by government entities, ten were developed by private/commercial companies, and one app was developed by a health organization.

Personal data collection

Our investigation found that these telehealth apps did not collect a significant amount of personal data. We observed three apps collecting an email address, phone number, and/or geolocation data, which is not unexpected considering the functionality they support.

We observed two privately-owned U.S. based apps (*Kencor COVID 19* and *98point6*) collecting the AAID. The collection of AAID information appears out of place because the AAID is an identifier that is used for advertising purposes.

Telehealth-specific features

Below are telehealth features we found that a user would expect in a telehealth app.

- **Viewing health data.** 13 of the 20 apps we tested allow users to view their health data, prescriptions, lab tests, and/or clinical notes.
- **Creating an appointment.** 12 apps allow users to create new doctor appointments.
- **Video calling.** 12 apps have enabled video capabilities for virtual appointments.

D. Quarantine Administration Apps

Quarantine administration apps are used in countries where governments strictly enforce quarantine and social distancing rules. These governments largely use these mobile apps to track the location of citizens and to ensure they are not interacting with others. Saudi Arabia, Russia, Poland, Colombia, India, and Nepal are the governments we observed deploying these apps.

Investigation limitations

Our team was able to detect and analyze 11 COVID-19 quarantine administration Android apps. However, we were not able to access all of the features in some apps as some required a local phone number to login. The full list of these apps can be found in **Appendix D**.

App developers and origins

Our team analyzed 11 apps that were developed in Saudi Arabia, Russia, Poland, Colombia, India and Nepal. Eight were created by government officials, while three were developed by private entities.

Our findings did not reveal willful misconduct with these apps, but we believe there should be greater transparency, accountability, and oversight to ensure governments are only using the information collected for purposes directly related to the pandemic.

III. Recommendations

If responsible steps to rein in the COVID-19 pandemic and reopen our devastated economy require changes in how much information people share about their health and movements, the public should be able to trust that their data will be used responsibly. Smartphone apps offer promising tools for collecting data about users' contacts and sharing that information with public health authorities.

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.

Our investigation revealed several instances in which apps fell short of best privacy and security practices and posed potential risks to users. In particular, some apps were not transparent about their data collection and third-party sharing practices; third-party SDKs that seemed extraneous to the functionality of the app were present in some apps; some apps sent transmissions that were not encrypted; and some apps requested permissions that have the potential to be collect more information than is necessary to accomplish the core functions for which the users were downloading the apps.

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.

To facilitate user trust, we encourage app developers to put privacy concerns at the forefront of their development efforts and embed privacy by design principles where possible. In particular, we recommend that developers ensure 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 about how users' personal data is collected, used, retained, stored, and shared.

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.

Appendix A - Contact Tracing Analyzed App List

	App	Country	Developer
1	Coronika - Your corona diary	Germany	Private
2	Private Kit	International	Private
3	Corona Watch	India	Government
4	TraceTogether	Singapore	Government
5	eRouška - part of smart quarantine	Czech Republic	Government
6	StopKorona!	Poland	Government
7	Hamagen (The Shield - The National App for Corona Virus War)	Israel	Government
8	Aarogya Setu	India	Joint
9	Mahakavach	India	Government
10	Care19	US	Private
11	Smittestopp	Norway	Government
12	ProteGO Safe	Poland	Government
13	Stopp Corona	Austria	Health Organization
14	Kenya Covid-19 Tracker	Kenya	Private
15	Corona Tracking and Response App	India	Government
16	Stop COVID-19 KG	Kyrgyzstan	Government
17	NICD COVID-19 Case Investigation	South Africa	Government
18	Healthy Together - COVID-19	US	Private
19	COVIDSafe	Australia	Government
20	Covid NP	Nepal	Government
21	COVID-19 Tracker by Medinin	India	Private
22	COVID Safe Paths	US	Private
23	Corona 360	France	Private

Appendix B - Symptom Checker Analyzed App List

	App	Country	Developer
1	patientMpower for COVID-19	Ireland	Private
2	Coronavírus - SUS	Brasil	Government
3	CDC	US	Government
4	NCOVI	Vietnam	Government
5	DDC-Care	Thailand	Private
6	BC COVID-19 Support	Canada	Joint
7	COVID AP-HM	France	Private
8	Covidom Patient	France	Health Organization
9	CoronaMadrid	Spain	Government
10	COVID-19.eus	Spain	Joint
11	STOP COVID19 CAT	Spain	Government
12	Asistencia COVID-19	Spain	Government
13	InNote Assistant	India	Private
14	Test Yourself Goa	India	Joint
15	COVID-19 Quarantine Monitor Tamil Nadu (official)	India	Joint
16	Covid-19	Italy	Private
17	LAZIOdrCovid	Italy	Government
18	98point6	US	Private
19	Kinsa for Wireless Smart Thermometers	International	Private
20	Self-Diagnosis - Ministry of Health and Welfare	South Korea	Government
21	Quarantine Watch	India	Government
22	ADiLife Covid-19	Italy	Private
23	COVID Symptom Tracker	International	Private
24	COVA Punjab	India	Government
25	Cova Punjab	India	Government
26	ProteGO Safe	Poland	Government
27	Stopp Corona	Austria	Health Organization
28	COVID-19MX	Mexico	Government
29	T COVID'19	India	Government
30	Bolivia Segura	Bolivia	Government
31	COVID-19 Gov PK	Pakistan	Government

32	Canada COVID-19	Canada	Government
33	Coronavirus UY	Uruguay	Government
34	CoronApp - Colombia	Colombia	Government
35	COVID Radar	Netherlands	Health Organization
36	Covid-19 Armenia	Armenia	Government
37	Sydney Care	US	Private
38	COVI	Qatar	Private
39	Sentinel Monitor (COVID-19 Management)	US	Private
40	FAMILY - COVID 19	Vietnam	Health Organization
41	Province 5 COVID-19 Tracker	Nepal	Government
42	Kencor COVID-19	US	Private
43	COVID-19 West Bengal Government	India	Government
44	Bharatpur Metropolitan | COVID-19 Response System	Nepal	Government
45	Speetar COVID-19	Libya	Private
46	NICD COVID-19 Case Investigation	South Africa	Government
47	SOS CORONA	Mali	Government
48	MUSC COVID-19 Vital Link	US	University
49	patientMpower for COVID-19 USA	US	Private
50	COVID-19 Tam	Mexico	Government
51	Castor COVID-19	US	Private
52	Healthy Together - COVID-19	US	Private
53	TN COVID -19 TELE CONSULTATION	India	Private
54	Covid NP	Nepal	Government
55	COVID-RD	Dominican Republic	Government
56	COVID19 - DXB Smart App	United Arab Emirates	Government
57	COVID-19 Tracker by Medinin	India	Private
58	COVID Control - A Johns Hopkins University Study	US	University
59	HowWeFeel: The How We Feel Project	US	Private
60	CoronaCheck	Pakistan	University

Appendix C - Telehealth Analyzed App List

	App	Country	Developer
1	Salud Responde	Spain	Government
2	GVA +Salut	Spain	Government
3	InNote Assistant	India	Private
4	Covid-19	Italy	Private
5	LAZIOdrCovid	Italy	Government
6	98point6	US	Private
7	Kinsa for Wireless Smart Thermometers	International	Private
8	ADiLife Covid-19	Italy	Private
9	COVID-19	Vietnam	Government
10	T COVID'19	India	Government
11	GVA Coronavirus	Spain	Government
12	Sydney Care	US	Private
13	Sentinel Monitor (COVID-19 Management)	US	Private
14	FAMILY - COVID 19	Vietnam	Health Organization
15	Province 5 COVID-19 Tracker	Nepal	Government
16	Kencor COVID-19	US	Private
17	TN COVID -19 TELE CONSULTATION	India	Private
18	TN HQ VC –NHM – DOCTORS APP COVID-19 S.O.S.	India	Private
19	COVID19 - DXB Smart App	United Arab Emirates	Government
20	COVID19 - DXB Responder	United Arab Emirates	Government

Appendix D - Quarantine Administration Analyzed App List

	App	Country	Developer
1	Quarantine Watch	India	Government
2	Mahakavach	India	Government
3	Home Quarantine (Kwarantanna domowa)	Poland	Government
4	Government services STOP Coronavirus	Russia	Government
5	Tawakkalna (Covid-19 KSA)	Saudi Arabia	Government
6	CoronApp - Colombia	Colombia	Government
7	CG Covid-19 ePass	India	Private
8	COVID-19 West Bengal Government	India	Government
9	Bharatpur Metropolitan | COVID-19 Response System	Nepal	Government
10	TN COVID -19 TELE CONSULTATION	India	Private
11	TN HQ VC –NHM – DOCTORS APP COVID-19 S.O.S.	India	Private