Supported by a grant from
OMIDYAR NETWORK

Colombia's CoronApp

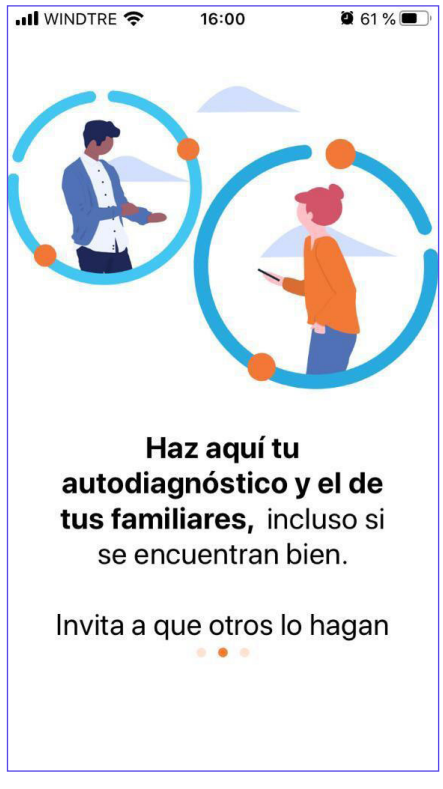
CoronApp is an app created by the Colombian government intended to monitor cases of Coronavirus in the country. The Colombian government has identified four main objectives for the initiative: (a) to facilitate healthcare for the worst-affected populations; (b) to identify epidemiological patterns in the worst-affected areas; (c) to develop geolocated analyses of the possible effects of the spread of the virus; and (d) to map the various affected populations by their location, gender, and age. The app is available for Android and Apple operating systems and has been downloaded almost 5 million times by May/2020), out of Colombia's total population of 50 million.

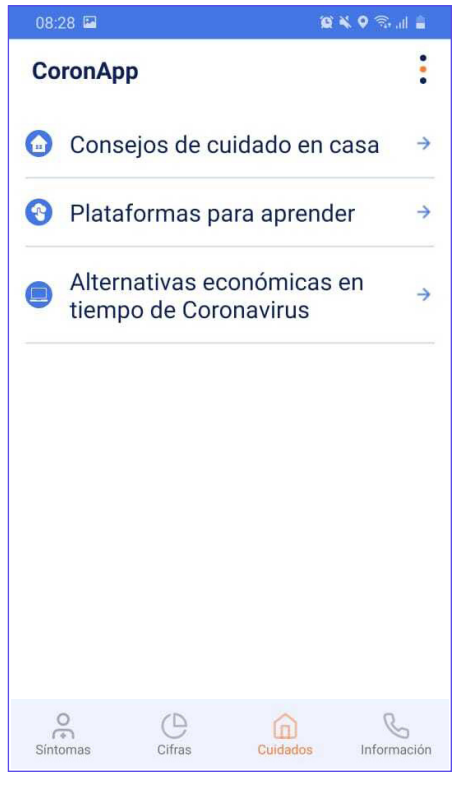
From the point of view of citizens, the main benefit of using the app is to be able to perform a self-diagnosis assessment and to receive recommendations for COVID's treatment[1]. From the government's side, the main benefit is to gather geolocalized health data generated by citizens, and to use it to support real-time decision-making.

Besides the self-diagnosis tool, the app also serves as an official access point to information of COVID activity in the user's region, and to allow users to apply for zero-rating plans packages during the crisis[2]. The Internet benefit can be used for any purpose, but because one has to register in the app to apply for it makes the CoronApp almost mandatory for low income citizens.

User registration in the app is optional for those seeking information only, but it is mandatory for those wanting to do a health self-assessment test. Identity data required during the registration process include the user's full name, national ID and a mobile number. However, the app usage also requires access to other sources of personal data, including WiFi and bluetooth phone records, what can be used to infer where the user is geolocalized, and who has been around the phone (i.e. contact-tracing records)[3].

In the app's Terms of Use (ToU)[4] it is stated that all information collected by the app are treated anonymously, and that all uses are done accordingly to the country's data protection framework. The ToU also sets data use restrictions, such as a limitation to use the data for health purposes and for the duration of the COVID-19 crisis only. The ToU also sets the app minimum age as 13-years old, meaning the app does collect data from minors between the ages of 13 and 18.





APPLYING THE FRAMEWORK

We apply below an evaluation test framework to understand the governance of digital identity systems. The framework was developed by the Center for Internet and Society (CIS), and it has been applied to other cases of digital identity in the past[5].

TEST SUMMARY

Broadly speaking, the CoronApp has limited performance in all three tests.

- The app operates without a clear legislative mandate. CoronApp was created by an executive ordinance resolution, and lacks legal definition of the its proper purpose and uses.
- The app has limited provision to rights-based principles such as data minimization, access to data and mitigation mechanisms. This means privacy and digital ID uses are potentially in danger.
- In terms of risk assessment, the app has no potential harms mapped. That means that in case of digital ID misuses, there is no plan of action in place.

1. RULE OF LAW TESTS

Below are most basic tests to ensure that a rule of law framework exists to govern the use of CoronApp.

1.1 LEGISLATIVE MANDATE

Is the use of digital identity system codified in valid law? For this test to be satisfied, the use must be codified in valid law — the parent legislation or other supporting legislation which is in accordance with the scheme envisioned by the parent legislation.

The legislative mandate backing the CoronApp is limited.

The app is not backed by an enacted law, being supported instead by an executive ordinance issued by the Ministry of Health (Resolution 666/2020)[6]. The executive ordinance, in turn, mentions two key legal frameworks to support the app's use, namely a constitutional provision for government initiative on health policies (namely Const. Art 2) and a federal law provision for health action (in specific, the Statutory Health Law, no. 1751/15). Specifically in terms of data protection legislation, there is no direct mention to the topic either in the law or in the executive mandate that supports the app. The only appearance for data protection legislation is in the app's Term of Use, that makes reference to the Habeas Data Law provisions (Law 1581/12).

By analysing the executive ordinance content, we also note that the CoronApp is only briefly cited in the text, without any further specification. The document's main topic deals with biosecurity protocol, being the CoronaApp referred to in articles 3.1.10 and 3.2.3. These articles make no indication of the conditions and circumstances in which the authorities are empowered to resort to the app, nor gives provisions against its abuse related to the collection, storage, use, or sharing of the digital ID information.

1.2 LEGITIMATE AIM

Does the law have a legitimate aim? For this test to be satisfied, the use of the identity data must fall under a legitimate aim.

The legitimate aim of the aforementioned executive ordinance is to promote and protect health.

Resolution 666/2000 states its aim as to promote "biosecurity protocol to mitigate, control and execute the adequate administration of the COVID-19 pandemic". This is aligned with the legal framework referred to by the app (i.e Art. 2 of the Constitution and the Statutory Health Law). Broadly speaking, both pieces of legislation are supportive of the app's general purpose.

1.3 DEFINING PURPOSES

Does the law clearly define the purposes for which the ID can be used for? For this test to be satisfied, the purpose for use and control of the identity data must be clearly specified through a legislative process.

The executive ordinance makes no mention to the specific purpose of the app, and provides no analysis of

how the legal mandate supports the app's purposes. Specifically in terms of Digital ID data, the Resolution makes no reference to the nature of data required to fulfil the app's legitimate aim, nor mentions eventual abuses related to surveillance, limit of personal data collection or retention.

1.4 DEFINING ACTORS

Does the law clearly define all the actors that can use or manage the ID? For this test to be satisfied, the actors who use and control the use of ID, must be clearly specified through a legislative process.

The Resolution focuses on defining the actors who can use or manage the app only. The document covers all actors involved in any organizations that deal with economic, social and public sector activities involved in biosecurity protocol, and is inclusive of any private or public individuals involved in such efforts. There are however no obligations or specific restrictions to actors using or managing the app in the Resolution.

1.5 REGULATING PRIVATE ACTORS

Is this use of the ID system by private actors adequately regulated? For this test to be satisfied, the use of ID by private actors is envisioned with adequate regulation.

The Resolution does not include provisions for private sector actors making use of the data, other than those involved directly in public sector activities.

1.6 DATA SPECIFICATION

Does the law clearly define the nature of data that will be collected? For this test to be satisfied, the use of identity data must be accompanied by clear specification of the personal data to be collected and processed.

The resolution does not define the nature of collected data or makes any mention to data specification. The Terms of Use only lists data collected during the registration purposes (i.e. users' name, government ID card number and phone number). This is however inconsistent to how the app technically works, and how the uses the government expects to make out of the collected app data. When using the app, for example, we identify that the app does ask permission to access other data from users, including the geolocation of the mobile phone, as well as access to WiFi and Bluetooth mobile records. When reviewing the uses the government plans to make out of the app, it is stated that the digital ID collected from users will be enriched with other data sources, as a way of profiling health data based on gender and age. All these information sources are not clearly listed in the app's Terms of Use.

1.7 NOTIFICATION MECHANISMS

Does the ID system provide adequate user notification mechanisms for this use case? For this test to be satisfied there must be user notification both for use and for any data breach.

The app's Term of Use has provision for setting a generic notification mechanism for data collection. The ToU makes reference to an email and phone number that can receive complaints and requests (Section 6), but apart from that brings no mention of procedural processes details, such as deadlines or administrative decision revision cases.

1.8 RIGHTS TO ACCESS

Do individuals have rights to access, confirmation, correction and opt out? For this test to be satisfied, individual holders' rights to their data are adequately guaranteed, even though they are not permitted to opt out of the system entirely.

The law provides generic provisions of rights to access. Section 6 of the Terms of Use mentions that data owners can confirm, correct and opt-out by contacting a government agency by email or phone indicated in the document, but provides no detailed mechanism for rights of access per se.

1.9 REDRESSAL MECHANISMS

Are there adequate civil and criminal redressal mechanisms in place to deal with violations of their rights arising from the use of identity data? For this test to be satisfied there is a need for adequate redressal mechanism whether is through the legislation governing this specific use, or through other laws such as the data protection law.

No redressal mechanism or access and correction of information is mentioned in the resolution. The Terms of Use states that in case of mediation of conflict, civil and criminal grievance should be addressed to the Republic of Colombia (Section 8).

2. RIGHTS BASED TESTS

This section identifies key rights-based principles related to privacy and digital ID use.

2.1 DATA MINIMIZATION

Are principles of data minimisation followed in the collection, use, and retention of personal data for this use case? For this test to be satisfied, there are rules in place to determine the appropriate amount of data to be collected and its retention period.

In general, the CoronApp does not address data minimization concerns.

The ToU lists personal data collected during the registration process (i.e. name, civil identification number and mobile number) only. There are however several other instances where personal data is collected, and which are not mentioned in the ToU.

During app's use, the user has to authorize access to phone location data, as well as WiFi and Bluetooth records. Sensitive information collected by the app is not described in detail in the ToU, which includes sensitive health information such as pre-existing pathologies and risk conditions. It is also possible that the user is sending information not only about its own behaviour, but also about those around it. All these cases go against data minimization practices.

Finally, CoronApp allows the user to register the health status of other family members. One user can do that by creating a new profile and completing the data for a third-party. This submission of personal data by others, without a validation of their express consent, is also a problem for data minimization practices.

2.2 ACCESS TO DATA

Does the law specify access that various private and public actors have to personal data in this use case? For this test to be satisfied there should be mandates to control access to data.

There is no definition in the ToU of who has access to data nor the conditions for actors doing so. The executive ordinance sets that only public service actors (or those acting on their activities behalf) can have access to the app. And that data use can only be done for health purposes, and during the COVID crises period. There is no provision for private sector access to data either, in the Resolution that created the app.

There are provisions however by how third parties can gain access to data storage and data processing. The ToU states that collected data can be accessed by third parties "that are required to improve the application, the use and consumption of [data]", and that "the information obtained from CoronApp can be shared or transferred for the purposes of health, statistics, generation of reports, among others".

Also, the ToU has no provision for destruction or anonymization of data, or mechanisms for how access to data will be interrupted. This is a major shortcoming for the app, who is designed to process data during the COVID crisis only.

2.3 EXCLUSIONS

Is the use of digital ID to access services exclusionary in this use case? For this test to be satisfied individuals should be allowed to use other forms of ID, as well as given greater say in controlling the access to their data.

The current version of the CoronApp allows users without registration to access basic health information provided by the app, including information on prevention measures, location of health services and reports on the coronavirus crises in Colombia.

The ToU states that users are responsible for access to the data network and for purchasing and updating compatible hardware or devices required to access and use CoronApp[7].

Official sources have stated that the app may become mandatory in the future to transit on the streets[8]. This functionality would be made possible through the generation of a QR code informing the users self-diagnosis status to be presented to others. This functionality is stated in the ToU (Section 9)

3. RISKS BASED TESTS

This section is centered on the perceived or existing risks related to privacy, welfare, equality and inclusion. Such risks usually have limited legal provision, though there is now an increasing focus on harm assessment in prominent frameworks such as the GDPR.

3.1 RISK ASSESSMENT

Is this use case regulated taking into account its potential risks? For this test to be satisfied the use of digital ID must be accompanied with proper risk assessment.

There is no publicly available information if the government has done a risk assessment before launching the app. Based on the limited legal provision we found, and the rights based analysis that shows few provisions for data protection, it is unlikely that a risk assessment test has been run before the app's release.

Running and releasing the app's Risk assessment would allow accounting for tangible harms to individuals, have clear provisions on prevention and appropriate recovery for harms if they occur. It should also take into account risks of profiling, surveillance, human execution errors, and unauthorized uses.

3.2 PRIVACY RISK MITIGATION

Is there a national data protection law in place? For this test to be satisfied there should be presence of a robust data protection framework that governs specific personal data to adequately reduces the risks.

In Colombia, there is in place a Personal Data Protection law 2012 (Law 1581/2012). In its Article 3, there is provision for information processing policies that are particularly central to the CoronApp. It states that "those responsible for the treatment must develop their policies for the treatment of personal data and to ensure that the Person in Charge of the Treatment is fully complying with the same". Therefore, there is provision for privacy risk mitigation provisions to be done before and during the CoronApp release.

3.3 DATA BREACH

For this test to succeed, privacy by design systems should be in place to minimise the harms from data breach.

In the ToU there is no specific mention to systems in place to minimize the harms from data breach. The ToU does mention aspects related to that, such as the provision to store health data in a dedicated data infrastructure, but ignores other clear liabilities, such as data encryption and data breach notification systems.

3.4 RESPONSE TO RISKS

Is there a mitigation strategy in place in case of failure or breach of the ID system?

There are no mitigation strategies to address failure of breach of the ID system, or the linking of personal data to sensible information related to users' healthcare data.

1. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126572:Abece-Todo-lo-que-debe-saber-sobre-CoronApp-Colombia-y-su-funcionamiento

2. https://id.presidencia.gov.co/Paginas/prensa/2020/descarga-CoronApp-Colombia-usuarios-telefonia-movil-prepago-obtendran-internet-minutos-voz-gratis-durante-un-mes-200424.aspx

3. https://web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/

4. We updated the app on 10 May 2020, and the findings in this report refers to the app version 1.2.40 and the Terms of Use included in the app until this date.

5. For a detailed description of the tests, see https://digitalid.design/evaluation-framework-02.html. For an applied version of the test in the health sector, see https://digitalid.design/evaluation-framework-case-studies/healthcare.html

6. https://id.presidencia.gov.co/Documents/200424-Resolucion-666-MinSalud.pdf

7. Mobile devices with Android 4.4 or higher operating system, and iOS 10.3 or higher operating system.

8. https://www.infobae.com/america/colombia/2020/04/15/como-funciona-la-aplicacion-del-gobierno-colombiano-que-sera-obligatoria-para-salir-a-la-calle/