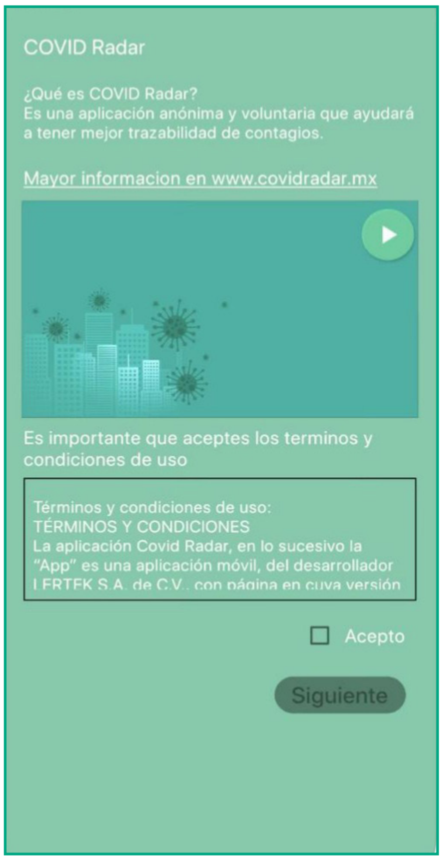
Supported by a grant from
OMIDYAR NETWORK

Mexico’s COVID Radar

During the COVID-19 crisis, the government of the Mexican state of Nuevo León launched the app called COVID Radar to monitor cases of coronavirus in the region. The app was developed by the private company Lertek, S.A. de CV, with the engagement of the Melissa Institute, a Chile-based private biotechnology research center, and *Alianza pelas Americas*, a transnational network of migrant-led associations across the Americas. *COVID Radar* was released for Android and Apple operating systems and has been downloaded almost 10,000 times by June/2020, out of the overall population of 5.12 million.

The main objective of the app is to alert citizens about possible contact with COVID-19 infected people. The main benefit for citizens using the app is its functionality in finding and alerting individuals who have been in contact with people infected with the new coronavirus. As for the government, the main objective is to identify people potentially exposed to the virus who should self-isolate, generate data of users’ encounters and enhance planning. During the launch of the app, the Nuevo León Secretary of Health stated that it functions on a voluntary basis, was developed using privacy by design and would not request geolocation data[1].

User registration is not mandatory for accessing the app, though users can share contact information, if they wish. Since identity data is not required during the registration process, the app can be used anonymously. For those that proceed with the registration, the app collects a wide range of personal data, including identifiable records, phone geolocation and health information.



COVID Radar

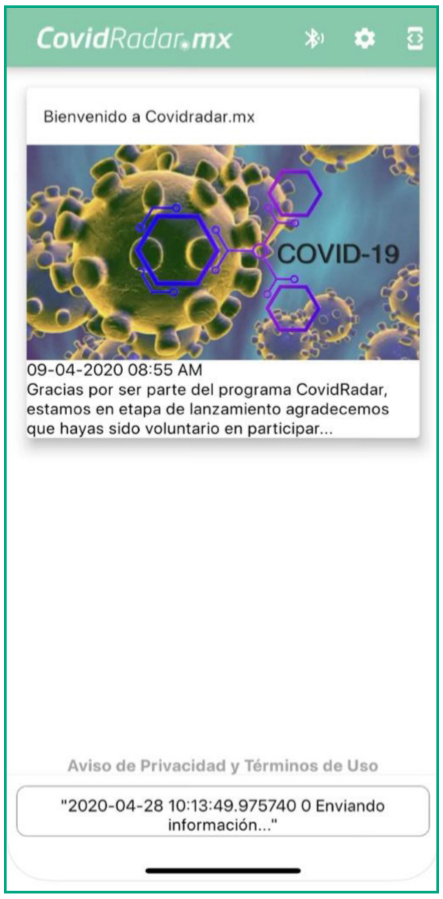
¿Qué es COVID Radar?
Es una aplicación anónima y voluntaria que ayudará a tener mejor trazabilidad de contagios.

Mayor informacion en www.covidradar.mx

Es importante que aceptes los terminos y condiciones de uso

Términos y condiciones de uso:
TÉRMINOS Y CONDICIONES
La aplicación Covid Radar, en lo sucesivo la "App" es una aplicación móvil, del desarrollador LERTEK S.A. de C.V., con página en cuya versión

□ Acepto

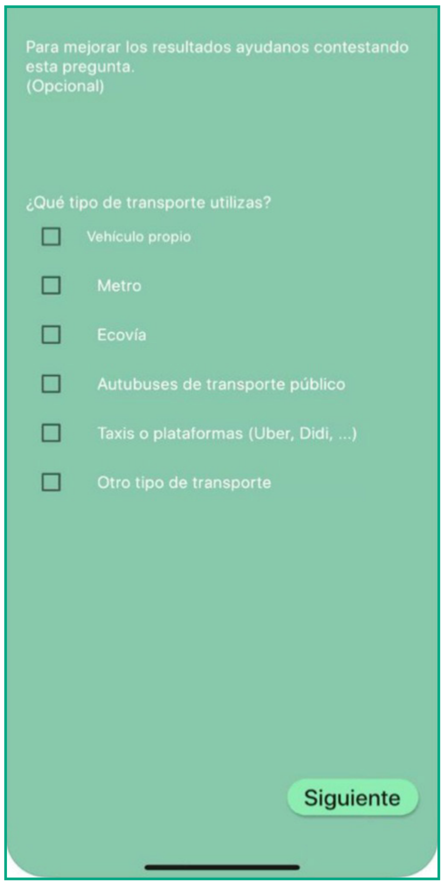


Bienvenido a Covidradar.mx

09-04-2020 08:55 AM
Gracias por ser parte del programa CovidRadar, estamos en etapa de lanzamiento agradecemos que hayas sido voluntario en participar...

Aviso de Privacidad y Términos de Uso

"2020-04-28 10:13:49.975740 0 Enviando información..."



Para mejorar los resultados ayudanos contestando esta pregunta.
(Opcional)

¿Qué tipo de transporte utilizas?

□ Vehículo propio

□ Metro

□ Ecovía

□ Autubuses de transporte público

□ Taxis o plataformas (Uber, Didi, ...)

□ Otro tipo de transporte

APPLYING THE FRAMEWORK

We apply an evaluation test framework below to understand the governance of digital identity systems, developed by the Center for Internet and Society (CIS). The test identifies the case study characteristics and its uses, and has been applied to other cases of digital identity in other regions, themes and contexts[2].

TEST SUMMARY

Broadly speaking, the *COVID Radar* app has a limited performance in all three tests.

» The app operates without a specific legislative mandate. We did not find any codified law or executive ordinance validating it. Nevertheless, users' personal data are broadly protected by the general Data Protection legislation.

» The app has some provision of rights-based principles, such as data minimization, specifications on access to data and mitigations mechanisms. The Terms of Use address data minimization and detailed security practices. However, there are no provision for destruction or anonymization of data when the limit period is over, therefore providing no mechanisms for when and how access to data will be interrupted.

» Regarding risk assessments, the app has no potential harms to individuals and society mapped.

LESSONS LEARNED

Broadly speaking the COVID Radar app has a limited legal mandate, some provisions of rights-based principles such as data minimization and no risk assessment. With this in mind, we highlight the following takeaways:

» **The lack of a specific legislative mandate backing the app is a risk for data protection. The government may consider regulating the application and making it open and publicly available.** Without a specific legal mandate, the basic and generic definition about the app's purpose and uses are subjected solely to the ToU's.

» **The ToU's specification is inconsistent about how the app technically works.** Although it states no personal or localised data is collected, the app does ask permission to access the geolocation data and WiFi and Bluetooth mobile records.

» **Even though the app is a regional government-adopted solution, the involvement of non-governmental organizations contributed to it in terms of privacy by design.** An important aspect is that the app's ToU is generally aligned with international privacy good practices for the development of contact-tracing applications.

» **A positive aspect of the app is that user registration is not mandatory for accessing any of its features.** By running anonymously, COVID Radar provides not only security to users, but also does not allow the profiling of individuals. That said, transparency on anonymization methodologies are fundamental. This is specially the occasion for highly sensitive health pandemic data. The ToU's mention this issue, but it should be as clear as possible.

1. RULE OF LAW TESTS

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

1.1 LEGISLATIVE MANDATE

Is the use of digital identity systems 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 *COVID Radar* is limited.

The app is not backed by an enacted law, nor any executive ordinance. The app does have a Terms of Use (ToU), which is insufficient as a supporting legislation requirement. That said, the ToU makes reference to key legal frameworks to support the app's use, namely the Federal Law on Protection of Personal Data Held by Private Parties ("the Law") and the General Law on Protection of Personal Data Held by Mandated Parties ("the Public Sector Law").

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 app cannot be defined, considering that it lacks a specific legislative mandate.

By analyzing the ToU, we infer that the app's aim is to control the spread of COVID-19 by using contact-tracing in mobile devices as a way to alert citizens about the possible contact with infected people, and identifying those citizens that require isolation. In spite of not having a formal legitimate aim, the ToU's reference to data collection and health issues indicates that the app is regulated by the country's data protection framework.

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.

There is no legal mandate defining the apps purpose and use.

Specifically in terms of digital ID data, there is no reference to the nature of data required to fulfill the app's legitimate aim, nor is there mention of eventual abuses related to surveillance, limit of personal data collection or retention.

In the ToU, the purpose of the app is clearly defined to minimize the spread of the virus. As stated in the document, the app's objective is to facilitate the detection of any person who has recently been in contact with a infected person both directly (family, friends and acquaintances) and indirectly, notifying them systematically and anonymously.

However, there is no clear indication regarding the intended period for data retention or even for the app's operation time.

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.

There is no available law defining the actors that can use or manage the ID, on the other hand the Terms of Use does.

The app's Terms of Use (ToU) has some limitations for those that can use the app (stating that minors must require parental authorization to download the app). Regarding what actors can manage the app, there is no specific mention, although, the document states that information will not be transmitted for commercial purposes of any nature in any case. It should be noted that the app is developed by a private company (Lertek S.A de CV), which is not defined in the ToU as an actor that can use or manage the ID data.

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.

There is no provision for actors using the data, either coming from the private or public sector. The ToU however states that the app is developed by the private sector company Lertek S.A. de C.V., and is run by the Nuevo León public sector agent (government).

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 ID must be accompanied by a clear specification of the personal data to be collected and processed.

There is no legal mandate defining the nature of collected data or making any mention to data specification. The Terms of Use states that neither personal nor localization data are collected.

The ToU's specification, however, is inconsistent to how the app technically works. When using the app, for example, we identified 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 states that COVID Radar registers dates, hour and collects Bluetooth records, as well as information on the operating system device, unique mobile identifier, and IP address.

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 a user notification mechanism both for use and for any data breach.

The app's Term of Use has a provision for a generic notification mechanism. The ToU makes reference to an email which users may resort to when in need of assistance, but apart from that brings no mention of procedural process details, such as deadlines or administrative decision revision cases. Also, the ToU defines that any changes in the ToU may occur, without prior consent or user notification.

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.

There is no legal mandate nor legal generic provisions of rights to access, nor in the app's Term of Use. This means that there is no provision for how users can confirm, correct and opt-out of the app's use, or how users can have access to rights of access mechanisms, for example. Even though, the General Law on Protection of Personal Data Held by Mandated Parties ensures those rights, it is not enough to foresee the right, but also to provide measures on how users can concretely exercise it.

1.9 REDRESSAL MECHANISMS

Are there adequate civil and criminal redressal mechanisms in place to deal with violations of individual rights arising from the use of identity data? For this test to be satisfied there is a need for an 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 any law, nor in the app's Term of Use.

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 minimization 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, COVID Radar does address data minimization concerns.

The users may use COVID Radar anonymously. When someone develops symptoms of COVID-19 and this information is updated in the applications, an alert is sent to other users who have been in contact with that person. For that, data collection is kept to a minimum for this functionality, consisting of Bluetooth records and permission to access device location. Nevertheless, the ToU does not define the duration that this data will be stored, processed and used.

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.

The ToU provides definition of who has access to data.

According to the document, authorities may be allowed access to the information collected, if required by law, in the exercise of any of its legal powers or by jurisdictional means, or on the grounds of any other of the exceptional cases contemplated by the General Law on Protection of Personal Data Held by Mandated Parties (namely articles, 22, 66 and 70) or by Federal Law on Protection of Personal Data Held by Private Parties (namely, articles 10 and 37). Also, the document states that the app is developed by the private sector company Lertek S.A. de C.V., and is run by the Nuevo León government. Due to this, the information would not be transmitted for commercial purposes of any nature in any case.

Despite the provision regarding access to data, the lack of indication on the period this data will be used deserves attention. As a point to be taken into account, there is no provision regarding whether the access to data is temporary or not, as well as no provision for destruction or anonymization of data when the limit period is over, therefore providing no mechanisms for when and how access to data will be interrupted.

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 COVID Radar is not mandatory and is available to all. The information on the app can be accessed anonymously. This means that those who do not have or do not want to share their identification are still included. It is noteworthy that even though Nuevo León State has one of the highest connectivity rates in Mexico and mobile devices have been increasingly used for that purpose, the region still has a huge population without Internet access.[3]

However, the app is conditioned to a device that has access to Bluetooth, internet or a data plan, as well as compatibility with iOS 8.0 and Android 5.0 or later versions. As stated in the ToU, these factors may influence the app's accessibility and performance.

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, although 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 stating that the government did a risk assessment before launching the app. Based on the limited legal provision we found, and the rights based analysis that shows few specific legal provisions for the app, it is unlikely that a risk assessment test was run before the app's release.

Running and releasing the app's risk assessment would allow accounting for tangible harms to individuals, and clear provisions on prevention and appropriate recovery mechanisms 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 the presence of a robust data protection framework that governs specific personal data to adequately reduce the risks.

In Mexico, the protection of personal data is a fundamental right recognised by the Constitution of Mexico since 2009. Additionally, the main legal frameworks for data protection are the Federal Law on Protection of Personal Data Held By Private Parties and the General Law on Protection of Personal Data Held by Mandated Parties.

In its Article 16, the Public Sector Law brings a provision for information processing policies that are particularly central to COVID Radar. It states that "the person responsible must observe the principles of legality, purpose, loyalty, consent, quality, proportionality, information and responsibility in the processing of personal data". Mexico also has in place a data protection authority (INAI) in charge of enforcing the Data Protection Laws.

Despite the robust legal framework in place, the app itself is not backed by a enacted law, which poses a privacy risk. Nonetheless, it is worth noting that the ToU's states that data is encrypted when transiting from the device to the server (indicating a centralized approach), but without giving specifications on its architecture.

3.3 DATA BREACH

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

The app's ToU points to a satisfactory system to minimize the harms from data breach. As stated, COVID Radar has physical, electronic, management and procedural security elements to protect and safeguard confidential information, such as the encryption of data from the device to the server, the limitation of data access to employees and authorized contractors that may need to access information to operate the app.

Also, while it acknowledges the liability that no security system can fully anticipate all potential security breaches, it ensures that continual efforts are made to protect the information by adopting reasonable, generally recognized and accepted security measures.

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 in the case of a breach of the ID system, or the linking of personal data to sensitive information related to users' healthcare data.

1. Manuel de la O Cavazos, Secretary of Health of Nuevo León stated the following during the launch of the application: *"Covid Radar es un programa voluntario y 100 por ciento anónimo, los usuarios pueden dejar sus datos de contacto en caso de desearlo y no requiere su geolocalización"*. See <https://www.forbes.com.mx/noticias-gobiernonuevo-leon-app-rastrear-casos-coronavirus-covid-19/>

2. 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

3. Retrieved from: <https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2019/internet2019_Nal.pdf>.