

## **The legal implications of contact tracing in Chile**

On February 26<sup>th</sup>, 2020, the first case of Covid 19 in Latin America was detected in Sao Pablo, Brazil. Countries throughout the region reacted by implementing a wide range of measures, reflecting national legislation, customs, and even ideology. The impact of those measures on personal privacy will have ongoing consequences throughout the region. One of the initiatives which have been most closely scrutinized is that of contact tracing.

In Chile, in mid-April the government rolled out a contact tracing app, called CoronApp. Other countries throughout Latin America have also announced tracing applications, including Argentina (March 22<sup>nd</sup>), Brazil (February 28<sup>th</sup>), Colombia (March 12<sup>th</sup>, also called CoronApp), Mexico (April 2<sup>nd</sup>) and Peru (April 3<sup>rd</sup>).

Although no information is available about how widely the app has been downloaded in Chile, there have been a number of concerns about its compliance with privacy regulations.

Privacy protection has been enshrined as a constitutional right in Chile since 2018. However, the actual privacy legislation dates back to 1999, and is in need of updating. Under national law, all data that can be linked to a specific individual is considered personal data, and consent is also required for its treatment. The law also considers “data regarding physical and mental health, as well as data regarding sexual activity” to be sensitive data, and as such can only be processed with the consent of the individual data subject, or when it is necessary for the determination or conveyance of health benefits.

That’s where the doubts regarding the CoronApp begin. The application, which is available on the Apple store and Google Play, is linked to the user’s government-issued personal identification number, which all Chilean and foreign residents must have. Through the app, users can report and control their own symptoms as well as those of people under their supervision, indicate where they’ll be quarantining, and communicate any circumstance that may put others at risk of infection. The app can also and record a user’s location and receive health updates from health authorities.

A first caveat is that users do not explicitly consent to the treatment of their personal or sensitive data. Though downloading and using the application is completely voluntary, it’s not clear that potential users are well informed of what it is they’re signing up for. The privacy policy, which can only be accessed before the app is registered to a specific user (or on the

Ministry's website) only "informs" users of how their data will be used, but does not require explicit consent of the user. Users are not even required to look at the privacy policy.

More worryingly, users can provide information on up to eight other people, and report their symptoms or other sensitive information, without any form of consent. This raises immediate and serious privacy concerns, as users could input data of other adults living with them or of children who are not under their legal guardianship. The privacy policy does state that the user is "responsible for the comprehensiveness, veracity, exactitude and precision" of third-party data that they input, but makes no attempt to compel users to obtain their consent.

Additionally, users get very little in return for exposing their private data. Since the app relies on self-reporting of symptoms, the government could use that information to single out individuals for quarantine or enforced testing, even without any actual medical data. There have already been cases of neighbors pushing back against medical professionals and others suspected of being infected, and this app could add to that discriminatory treatment. If the intention is that the app can refer people showing symptoms to local health services, that could be achieved by listing known symptoms and identifying health providers in the vicinity of the user, without collecting personal information beyond their location.

Doubts have also been expressed about how the government processes and stores the data provided by CoronApp users. The privacy policy states that all information registered on the app will be stored and replicated on Amazon Web Services in the US-East Region, physically located in the state of Virginia, but no indication is given about safety or confidentiality measures. There is a broad reference to the data being treated as required by Chilean law, but there is no mention of how American regulations may also affect its storage and access.

The policy also says that only the Ministry of Health and "other sanitary bodies authorized by law" may access the provided data, but goes on to say that the Ministry may transfer data to third parties "based on a judicial or administrative order". This is broad enough that there is very little chance that users will know beforehand who may end up accessing their information.

In an apparent contradiction to the above, the app also states that user data can be transferred to third parties with which the Ministry signs cooperation agreements "for purposes compatible with those declared and consented to by the user". These third parties must only take care to anonymize the data if they intend to publish the result of their analysis, implying that they will receive and use all personal and sensitive data intact. If they decided to sell that data to private health or pharmaceutical companies, which in theory could be construed as "purposes compatible" with those of the app, there would be very little that users could do.

Finally, the app declares that users' data will be used and treated "as long as needed to protect public health, in the context of the medical emergency", but authorities could make a strong case that, short of total eradication of Covid-19, data on this outbreak should be on hand to treat future events, indefinitely. And given the loose restrictions on transfer to third parties,

that information could eventually be sent to “compatible” private companies, such as insurers and employers.

In short, while contact tracing can be a valuable tool for abating the spread of the virus, greater attention should be given to the protection of user privacy, to ensure that the implicit dangers of revealing private information do not outweigh the potential benefits of the app. Authorities should also be mindful that many of the most vulnerable members of the population, including seniors and lower-income citizens who are more exposed to underlying medical conditions, may very well not have the means to access the digital technology needed to run the application.

Sources:

<http://virological.org/t/first-cases-of-coronavirus-disease-covid-19-in-brazil-south-america-2-genomes-3rd-march-2020/409>

<https://www.pauta.cl/ciencia-y-tecnologia/gobierno-de-chile-lanza-primera-app-covid-19-llamada-coronapp-hay-criticas>

<https://www.latercera.com/que-pasa/noticia/asi-es-coronapp-la-aplicacion-del-gobierno-de-chile-para-ayudar-a-combatir-el-coronavirus/15TDWD4JPEFW5EG7FTIJWZEJAU/>

<https://ciperchile.cl/2020/04/22/problemas-de-proteccion-de-los-datos-personales-de-la-aplicacion-coronapp/>

<https://www.derechosdigitales.org/14301/civil-society-from-latin-america-and-the-caribbean-demands-to-respect-human-rights-when-governments-deploy-digital-technologies-to-fight-against-covid-19/>

[https://colombia.as.com/colombia/2020/04/16/tikitakas/1587004974\\_964430.html](https://colombia.as.com/colombia/2020/04/16/tikitakas/1587004974_964430.html)

<https://gestion.pe/peru/coronavirus-peru-lanzan-nueva-version-de-aplicacion-peru-en-tus-manos-para-advertir-zonas-de-contagio-cuarentena-estado-de-emergencia-covid-19-nndc-noticia/>

<https://hipertextual.com/2020/04/mexico-app-coronavirus-ios-android>

<https://www.ambito.com/informacion-general/coronavirus/como-funciona-cuidar-la-nueva-app-argentina-n5098539>