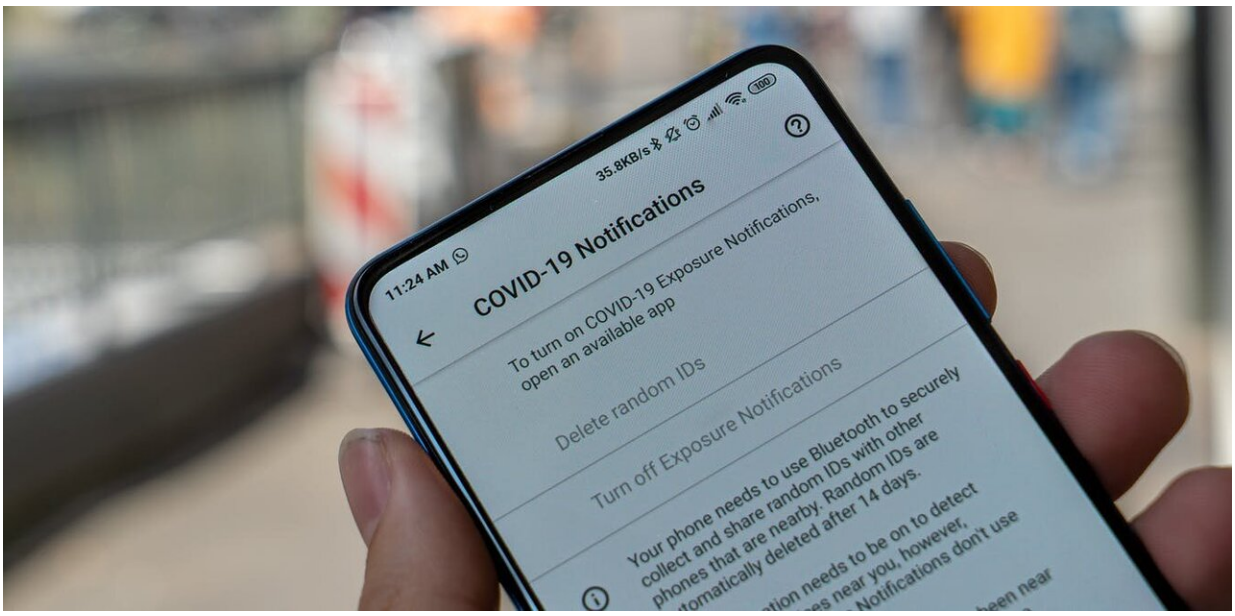
Privacy, perceptions and effectiveness: the challenges of developing coronavirus contact-tracing apps

July 22 2020, by Roxana Ologeanu-Taddei



Are you ready to start sharing your personal information with an app developed by Google and Apple? CC BY

To control the spread of the COVID-19 pandemic, more than 50 countries have implemented applications to trace the contacts of people who may be infected.

The installation and use of these applications are voluntary in the

majority of countries, but in others they're mandatory. China is a notable example, but use of the application is also required in countries such as India, Indonesia and Vietnam. In Turkey, those who have been infected with the virus are required to download the application, which shares information with security forces.

Even in fully democratic countries that promise that users' data will be kept private—for example in the Netherlands and France – there are concerns that the application could be used as a surveillance tool.

Identity and privacy

Beyond the cultural and political differences between countries, two main points are at stake when it comes to privacy:

- Users' identities: Most countries have implemented an anonymization or pseudonymization approach, which can be fulfilled by the Bluetooth connection. The few countries that opted for an approach that does not respect privacy, such as Kuwait, have implemented a geolocation app.
- Data structure and storage: All applications require a data architecture—the internal structure for recording, storing and processing information—and developers must choose between a centralized or decentralized approach. With a centralized architecture, data is uploaded to a server controlled by the government health authority rather than stored locally on users' devices.

France's StopCovid application uses a centralized architecture, while Germany finally adopted a decentralized approach developed by Google and Apple, inspired by the technique developed by the European consortium Decentralized Privacy-Preserving Proximity Tracing (DP-3T). The United Kingdom adopted a centralized approach but,

facing increased criticism about the risk to privacy raised by its centralized app, switched to the Google-Apple technique. Countries as Japan and Italy made the same choice.

A second question relates to Bluetooth-based applications' effectiveness in fulfilling the objective pursued. For example, depending on environmental factors, a device could estimate that another is 20 meters away… or 2. Because accurately estimating physical proximity and contact time are essential, any additional level of uncertainty can greatly diminish such applications' effectiveness.

Perceptions matter

This is important not only in terms of functionality, but also because it has an impact on users' perceptions. In countries where the applications are voluntary, if fewer people think an application is effective, the lower the adoption will be and, in turn, the lower the utility. If potential users' perceptions are more positive, they're more likely to install and use the application, and the more useful it will become for others. (This is known as the principle of network externalities.) Like the telephone, even the best application cannot be useful and efficient if it is used by only one person. Instead, usefulness depends on the incentives and benefits that users can expect. Beyond the public health objective, users could have access to analytics or relevant information to protect themselves from the virus.

A third point is technical performance. Several apps were criticized for bugs, low performance or poor compatibility with iPhones, as with Australia's COVIDSafe. These and other issues were reviewed by the independent Ada Lovelace Institute in in United Kingdom.

Such challenges are well known to managers of corporate information systems. On one hand they are the guarantors of secure access and

consequently implement centralized information technologies. On the other, employees are increasingly use their personal telephones and applications originated in the consumer market, such as WhatsApp, and the massive boost in distance work during the epidemic as amplified the trend.

IT managers want to maintain control over the devices and applications used for work, yet employees consider consumer-focused applications to be more efficient, better performing, and more enjoyable than corporate technologies. As with contact-tracing applications, the main issue here is how to implement a governance taking into account individuals' voices and concerns.Responding on employees' needs and expectations, corporate-based technology also provides now availability across borders, and thus facilitates professional and personal mobility.

GAFAM to the rescue?

Control is indeed the main issue at stake in the current choices for coronavirus contact tracing applications. Regardless of the country, there are governments and health agencies that want to control or even centralize data. Thus, the majority of them have opted for centralized systems developed at the national level, in a similar way to corporate information systems. As noted, several applications have been criticized for this choice as well as for technical problems.

It is interesting that Google and Apple have proposed an application that is perceived as being more reliable and providing increased security and privacy through anonymization and decentralized architecture. Given the dominance and control that these GAFAM firms exert, one might expect them to be less concerned about users' privacy than governments. Is because Apple and Google are more virtuous than public health decision-makers?

In fact, the answer is more pragmatic: Apple and Google are talking to consumers, and therefore take their interests and needs into account—at least superficially. They know that the success of their applications relies on user adoption, and that that this adoption would be compromised if the applications developed compete with those implemented by governments. Thus, they offer access to their application programming interfaces (APIs) to each country that wishes to implement the application. This allows countries to configure them as they wish, in particularly concerning privacy issues.

Learning to listen to citizen-consumers

Policymakers seem to have forgotten that they too must address their citizen-consumers—it's not just about the centralized control of health data. Citizens' fear of tracking by authorities or company managers may even be greater than the fear of tracking by Google and Apple for marketing purposes. Therefore, policymakers should reinvent the governance of apps for health and overall for social purposes.

It is should be noted that when coronavirus contact tracing apps are developed, it is generally experts in data privacy or representatives of various public bodies that are consulted. To my knowledge, only Switzerland conducted an opinion poll asking citizens what their attitudes were about such an applicationand 70% of respondees backed the application.

Efforts to educate and learn from citizens and residents about the issues of such apps should be encouraged and used for decision-making. It's also essential for policymakers to incorporate and emphasis customer experience in employee and citizen experiences. This is not only a matter of adoption but also, more generally, of establishing trust in decision makers, be they in firms or the government.