Use of apps in the COVID-19 response and the loss of privacy protection

Mobile apps provide a convenient source of tracking and data collection to fight against the spread of COVID-19. We report our analysis of 50 COVID-19-related apps, including their use and their access to personally identifiable information, to ensure that the right to privacy and civil liberties are protected.

Tanusree Sharma and Masooda Bashir

Compared with prior infectious-disease outbreaks (e.g., the 'Spanish flu' pandemic of 1918 and the 'Asian flu' pandemic of 1957), the COVID-19 emergency is occurring in a vastly more connected and digital world. Governments in multiple countries are pushing for location surveillance to contain the spread of COVID-19[1]. Digital surveillance may be the most effective way to contain the spread of the outbreak, but how privacy rights may be impacted must be considered both now and as this crisis moves forward. Fear and uncertainty often win out over civil liberties; however, as has been learned from past crises, such as the terrorist attacks of 11 September 2001, it can be hard to regain lost liberties[2]. Thus, it is critical not only that virus-response opportunities provided by technology be embraced but also that technology be used to ensure that the right to privacy is secured (Fig. 1).

Some countries, such as China, Israel, Singapore and South Korea, have launched tracking apps to fight the pandemic, and many more commercial apps have been released since the beginning of the outbreak. Here we examine 50 apps available in the Google Play Store that have been developed specifically for COVID-19 (Supplementary Table 1).

The most common functionalities of the apps are as follows: live maps and updates of confirmed cases; real-time location-based alerts; systems for monitoring and controlling home isolation and quarantine, direct reporting to government, and self-reporting of symptoms; and education about COVID-19. Some more-advanced services include self-assessment of daily physiological status; monitoring of vital parameters, such as temperature, heart rate, oxygen and blood pressure, through the use of Bluetooth-enabled medical devices; virtual medical consultations (ADiLife Covid-19 in Italy); social science–based interventions based on predictive analysis of diseases in specific locations (OpenWHO); and community-driven contact tracing (TraceTogether and mfineRadar).

We found that 30 of the 50 apps require permission for numerous types of access to users' mobile devices. For example, some demand access to contacts, photos, media, files, location data, the camera, the device ID, call information, the WiFi connection, the microphone, full network access, the Google service configuration, and the ability to change network connectivity and audio settings, to name just a few types of access.

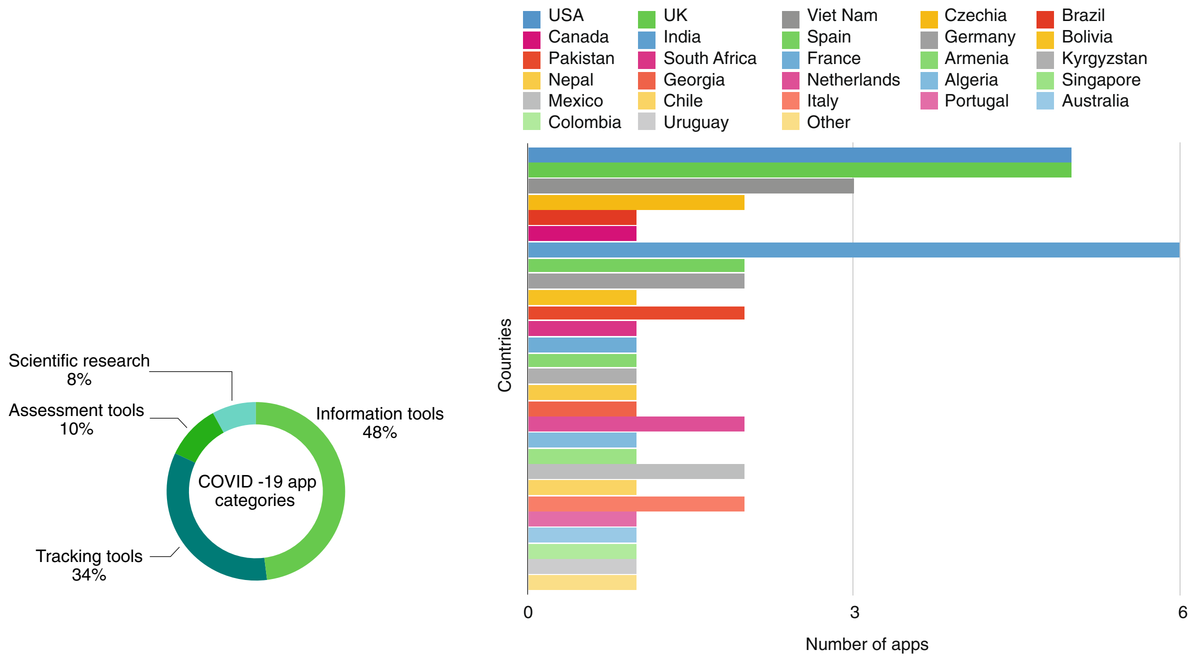

Fig. 1 | Data dashboards of COVID-19 apps. The distribution of COVID-19 apps (data collected from Google Play Store).

In addition, some apps explicitly state that they will collect information about the person's age, email address, phone number and postal code; the device's location, unique device identifiers, mobile IP address and operating system; and the types of browsers used on the mobile device.

A troubling discovery is that only 16 of the 50 apps indicate that the user's data will be made anonymous, encrypted and secured and will be transmitted online and reported only in an aggregated format. Our data represent a number of government-issued COVID-19 tracing apps that are from both developing countries and developed countries. Somewhat worryingly, 20 apps from our sample were issued by governments, health ministries and other such official sources. While the US government is not currently requiring citizens to download any tracking apps, there are apps in the Play Store that were developed by US healthcare providers (Sentinel Healthcare, 98point6 and HealthLynked) that have similar functionalities. What is not clear is whether any of the data collected are protected by any laws or regulations such as the Health Insurance Portability and Accountability Act or electronic protected health information.

It is, therefore, no surprise that Albert Fox Cahn, Executive Director of the Surveillance Technology Oversight Project (https://www.stopspying.org/), a nonprofit organization in Manhattan, New York, said "We could so easily end up in a situation where we empower local, state or federal government to take measures in response to this pandemic that fundamentally change the scope of American civil rights"[3]. What is disconcerting is that these apps are continuously collecting and processing highly sensitive personally identifiable information, such as health information, location and direct identifiers (e.g., name, age, email address, and voter/national identification). Governments' use of such tracking technology — and the possibilities for how they might use it after the pandemic — is chilling to many. Notably, surveillance mapping through apps is allowing governments to identify people's travel paths and their entire social networks[4].

The European Data Protection Board issued a statement on the importance of protecting personal data while fighting COVID-19[5] and flagged articles of the General Data Protection Regulation that provide the legal grounds for processing personal data in the context of epidemics[5]. In the USA, however, there is no structured or legal privacy framework in place. The only federal agency that oversees digital privacy protections is the Federal Trade Commission, which addresses mainly inconsistent privacy policies from the point of view of consumer protection.

In recent weeks, US President Donald Trump assembled representatives from a number of digital-technology companies to formulate how mobile location data could be used to track citizens to address the pandemic in the USA[6]. In parallel, privacy and security researchers are working tirelessly to propose protection mechanisms that may be useful. For example, a recent publication by Harvard University's Center for Ethics identifies tracing protocols that mitigate privacy risks and promotes the use of critical security and privacy controls that can accelerate medical responses while maintaining people's rights[7]. Another group of researchers has proposed a system for secure and privacy-preserving proximity tracing at large scales through the application of anonymous identifiers and functional requirements of fundamental security and privacy, such as data minimization and retention[8]. Other emergency publications have suggested anonymization with random 'noise'[9], artificial intelligence–generated 'noise' or additively homomorphic encryption and message-based methods[10] to generalize people's data while being able to protect users' privacy.

Healthcare providers must absolutely use whatever means are available to save lives and confine the spread of the virus. But it is up to the rest, especially those in the field of information privacy and security, to ask the questions needed to protect the right to privacy. However, it is important to note that there may be no choice but to adopt such mass surveillance measures if this pandemic does not go away or if another one comes into existence. Thus, it is crucial to ensure that policies, mathematical models and technological measures are developed to protect the data that are being collected and used, and transparency must be promoted in how data can help contain the spread while ensuring that civil liberties will still be protected.

Tanusree Sharma [1]✉ and
Masooda Bashir [2]✉

[1]Illinois Informatics Institute, University of Illinois at Urbana-Champaign, Champaign, IL, USA. [2]School of Information Sciences, University of Illinois at Urbana-Champaign, Champaign, IL, USA.
✉*e-mail: tsharma6@illinois.edu; mnb@illinois.edu*

Published online: 26 May 2020
https://doi.org/10.1038/s41591-020-0928-y

References

1. Ting, D. S. W., Carin, L., Dzau, V. & Wong, T. Y. *Nat. Med.* **26**, 459–461 (2020).
2. Kahn, F. S. *Tulane Law Rev.* **6**, 1579–1644 (2002).
3. Singer, N. & Choe, S.-H. *The New York Times* https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html (23 March 2020; updated 17 April 2020)
4. *The Economist* https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic (26 March 2020).
5. European Data Protection Board. https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en (16 March 2020).
6. Lomas, N. *TechCrunch* https://techcrunch.com/2020/03/20/what-are-the-rules-wrapping-privacy-during-covid-19/ (2020).
7. Hart, V. et al. *Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks* (Edmond J. Safra Center for Ethics, 2020).
8. Troncoso, C. et al. https://github.com/DP-3T/documents (2020).
9. Cho, H., Ippolito, D. & Yu, Y. W. Preprint at *arXiv* https://arxiv.org/abs/2003.11511v2 (2020).
10. Bell, J., Butler, D., Hicks, C. & Crowcroft, J. Preprint at *arXiv* https://arxiv.org/abs/2004.04059 (2020).

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41591-020-0928-y.