Medicine, Harvard Medical School, Boston, MA, USA. [36]*Department of Pulmonary Medicine and Critical Care, Massachusetts General Hospital (MGH), Boston, MA, USA.* [37]*ETH Zurich, Department for Computer Science, Zurich, University Hospital Zurich, Medical Informatics, Zurich and SIB Swiss Institute of Bioinformatics, Zurich and ELLIS Unit, ETH Zurich, Switzerland.* [38]*Science for Life Laboratory (SciLifeLab), Department of Immunology, Genetics and Pathology, Uppsala University, Uppsala, Sweden.* [39]*Department of Pathology and Laboratory Medicine, Weill Cornell Medicine, New York, NY, USA.* [40]*King's College, London, UK.* [41]*Science for Life Laboratory (SciLifeLab), Department of Microbiology, Tumor and Cell Biology, Karolinska Institutet, Stockholm, Sweden.* [42]*Luxembourg Centre for Systems Biomedicine, University of Luxembourg, Esch-sur-Alzette, Luxembourg.*
✉*e-mail: eran.segal@weizmann.ac.il*

Published online: 2 June 2020
https://doi.org/10.1038/s41591-020-0929-x

References

1. Tariq, A. et al. *medRxiv* https://doi.org/10.1101/2020.02.21.20026435 (2020).
2. Smolinski, M. S. et al. *Am. J. Public Health* **105**, 2124–2130 (2015).
3. Tian, H. et al. *Science* **368**, 638–642 (2020).
4. Guan, W.-J. et al. *N. Engl. J. Med.* **382**, 1708–1720 (2020).
5. Wu, Z. & McGoogan, J. M. *JAMA* **323**, 1239–1242 (2020).
6. Adalja, A. A., Toner, E. & Inglesby, T. V. *JAMA* **323**, 1343–1344 (2020).
7. Gudbjartsson, D. F. et al. *N. Engl. J. Med.* https://doi.org/10.1056/NEJMoa2006100 (2020).
8. Mizumoto, K., Kagaya, K., Zarebski, A. & Chowell, G. *Eurosurveillance* https://doi.org/10.2807/1560-7917.ES.2020.25.10.2000180 (2020).
9. Sutton, D., Fuchs, K., D'Alton, M. & Goffman, D. *N. Engl. J. Med.* https://doi.org/10.1056/NEJMc2009316 (2020).
10. Rossman, H. et al. *Nat. Med.* **26**, 634–638 (2020).
11. Drew, D. A. et al. *Science* https://doi.org/10.1126/science.abc0473 (2020).
12. Menni, C. et al. *Nat. Med.* https://doi.org/10.1038/s41591-020-0916-2 (2020).
13. Dankar, F. K. & El Emam, K. *Trans. Data Priv.* **6**, 35–67 (2013).
14. King, G. & Lu, Y. *Stat. Sci.* **23**, 78–91 (2008).

Acknowledgements

The CCC is a nonprofit consortium open to anyone who shares the vision of making data available to help the public good and fight COVID-19; as of May 2020 participating countries are Argentina, Canada, Estonia, Germany, Israel, Luxembourg, Macedonia, Slovenia, Sweden, Switzerland, UK and USA. There are no membership fees. Please contact us at info@coronaviruscensuscollective.org if you are interested in joining.

Competing interests

The authors declare no competing interests.

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. 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

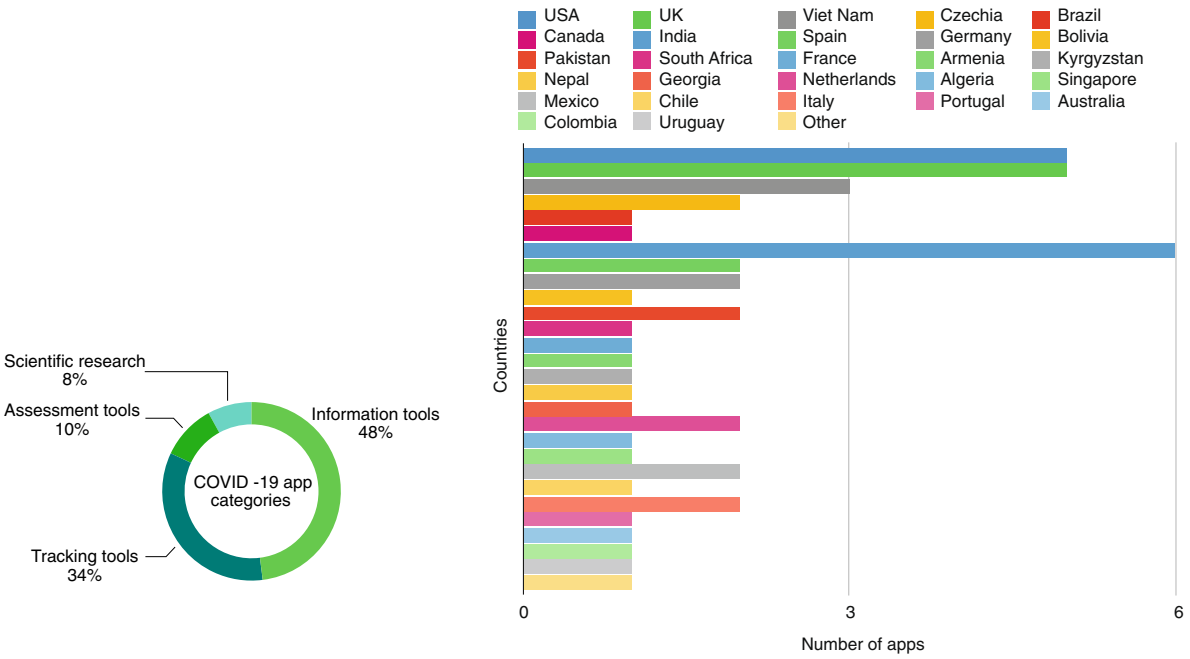

Fig. 1 | Data dashboards of COVID-19 apps. The distribution of COVID-19 apps (data collected from Google Play Store).

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.

Mass-surveillance technologies to fight coronavirus spread: the case of Israel

As the COVID-19 pandemic escalates, teams around the world are now advocating for a new approach to monitoring transmission: tapping into cellphone location data to track infection spread and warn people who may have been exposed. Here we present data collected in Israel through this approach so far and discuss the privacy concerns, alternatives and different 'flavors' of cellphone surveillance. We also propose safeguards needed to minimize the risk for civil rights.

Moran Amit, Heli Kimhi, Tarif Bader, Jacob Chen, Elon Glassberg and Avi Benov

On 16 March 2020, the Israeli government approved two emergency regulations allowing mass location tracking of citizens as part of the national effort to slow the pandemic of coronavirus disease 2019 (COVID-19). At that point, the Israeli health system, which serves a population of 8.7 million people, was facing 255 cases of confirmed infection with the causative coronavirus SARS-CoV-2 and 5 COVID-19-related deaths. Two weeks later the number of new cases started dropping from nearly 800 per day to approximately 500 per day, and it has continued to decrease, to fewer than 100 new cases per day (as of 2 May 2020). This was accompanied by plateaus in the total number of cases and the number of active cases. As of 9 April 2020, this had led to a near-equilibrium between the number of newly infected patients and the number of recovered and discharged patients each day[1].

The new regulations served two purposes: (1) enforcing new social isolation rules, and (2) tracking the locations of patients infected with the virus. Countries such as Taiwan and Singapore have authorized law-enforcement authorities to monitor quarantine orders remotely. However, Israel is the only country to implement 'digital epidemiological investigation' to track down potential contacts of infected individuals[2]. The mission was assigned to Israel's domestic security agency, the Israel Security Agency (ISA). Usually, the ISA's primary mission is to thwart terrorism and espionage. However, the agency's advanced digital surveillance capabilities have been redirected to allow comprehensive epidemiological investigation and the digital identification of people who have come into contact with infected people. Decision-makers explained this unprecedented step by citing the acute need to conduct hundreds of investigations in a short period to allow quarantine of possibly infected but asymptomatic people and prevent further contagion.

The fairly high reproduction number (R_0) of SARS-CoV-2 (1.4–3.9)[3] has rapidly exhausted the capacities of most public-health systems to perform traditional epidemiologic investigations in a timely fashion[4]. Owing to the rapid spread of the virus, along with the limitations of human memory (such as recall bias) and the inability to identify interactions with people that one does not know, it is impossible to monitor with high accuracy the contacts of an infected person. Hence, applying intelligence technologies to collect data on the civilian population could be a useful measure for lessening the spread of the disease. Nevertheless, the implications of such a move for personal privacy are far-reaching and might last long after the COVID-19 pandemic subsides.

After the regulations allowing digital contact tracing were approved, the ISA started using a cache of mobile-phone-location data to help identify people who had crossed paths with patients who had positive SARS-CoV-2 tests. Close contacts of patients were put into mandatory quarantine to stop further contagion. One week after the initiation of coronavirus surveillance, the Israeli Ministry of Health reported that extensive traditional epidemiological investigations had revealed only one third of known potential spreaders (6% of whom were infected individuals and 27% their contacts), while the digital surveillance program identified the remaining contacts (67%)[5]. Three days later, the ISA reported that approximately 40% of overall patients with confirmed SARS-CoV-2 in Israel had been identified through the digital surveillance measures. One month after the implementation of the mass-surveillance program for contact tracing, the Supreme Court of the state of Israel, in response to a petition submitted by human rights organizations, journalists and others, discussed the need for a middle ground to guard against the violation of basic human rights. During this discussion, Ministry of Health representatives reported that out of 12,501 confirmed cases in Israel, 4,611 (36.8%) cases had been detected through cellphone tracking[6]. Given the number of 'imported' cases (i.e., cases carried by travelers from overseas rather than local transmissions), the detection rate of cellphone tracking was nearly 50%. Of note, the health officials reported a false-positive rate of 5%; to minimize the impact of this false-positive rate, the system developers added a feature that allows people to appeal if they feel that their localization data were wrong. The Supreme