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

Box 1 Principles for maintaining privacy and civil liberties with cellphone tracking

Time: The program should be limited in time, and the need for digital surveillance should be continually re-evaluated. A contact-tracing app might have relatively little impact in a city in which a high volume of coronavirus cases and extensive community transmission have already shuttered businesses and forced citizens inside. Mass surveillance is most potent at the time of crisis entry or in the transition to a new steady state, when isolating potential cases could avert the need to shut down all schools and businesses.

Operator: Civilian operators (such as the telecommunication and software industries) should be advised of, and preferably operate, the mass contact-tracing systems. When the only available system is military, it should be activated by primary legislation that defines its temporal limitations and reporting requirements. Military technologies are designed to neutralize manmade threats; thus, intelligence agencies operate in secrecy. In contrast, civil scenarios such as SARS-CoV-2 require transparency. Legislation to prevent a 'slippery slope' and the illegitimate use of military technologies against citizens is needed.

Data: The public should know what data are collected and how those data will be used, stored and shared. The type of data should be scientifically justified and no more intrusive to civil liberties than necessary—the principle of 'data minimization'. Data should be made anonymous to avoid unmasking and stigmatizing of infected people and the businesses they frequent. Epidemiologists should define time limits for data storage; at the end of this predefined period, the data should be deleted.

Access: Data access should be permitted to as few people as possible. Access should be secured by a second step of identity verification to prevent accidental entries of unauthorized staff. Access to the database should be monitored continuously. All authorized personnel should be required to have security clearance and sign a nondisclosure agreement. Distribution of raw location data should be limited to authorized personnel; law-enforcement authorities should receive action orders only, rather than access to the contact-tracking tool or raw data files.

Participation: Technology can save lives, but if its implementation unreasonably threatens privacy, more lives may be at risk. Preferably, governments should encourage voluntary participation, and device users should consent to the use of their data. Authorities should take any action needed to augment transparency and protect individual privacy; this, in turn, will increase voluntary participation in the digital tracking program.

Supervision: Redirecting instruments designed for counterterrorism operations toward the civilian population requires the highest level of supervision and transparency. An independent committee of professionals should be established to monitor the program daily. This committee will include privacy law attorneys, ethicists, epidemiologists, a digital privacy expert, and a public representative.

Court ruled that primary legislation will be required before the use of global contact-tracing technology can be extended during the transition period as part of the 'exit strategy'[7]. Importantly, so far, the policy in Israel indicates self-quarantine on a case-by-case basis for those at high risk of exposure; quarantine is not universal. In accordance with the Supreme Court's decision, on 5 May 2020, the Israeli parliament approved a 3-week extension of the emergency regulations, including digital contact tracing by the ISA. This will allow enough time for the Israeli government to pass the primary legislation required for cellphone tracking to control the spread of SARS-CoV-2[8].

These encouraging results raise a fundamental question about how to balance the need for a non-voluntary emergency mass-surveillance program against the risk of permanent damage to civil liberties during regular times. At present, US officials are in active discussions with technology giants such as Facebook and Google, as well as public-health experts, about how to harness technology to stem the SARS-CoV-2 outbreak. Mobile-phone data represent an obvious option for this purpose because they provide real-time information on people's movements. However, privacy advocates are raising concerns about the practice of using and sharing people's personal data during a global health crisis and advise caution when tracking the movements of patients with COVID-19 or those infected with the new coronavirus. Both authorities and the public will have to weigh the value of privacy against the possibility that data collection could save millions of lives.

In countries with strict data privacy laws, one option for collecting data is to ask telecommunications companies to share anonymous, aggregated information they have already gathered. Mobile carriers in Germany and Italy have started to share mobile-phone-location data with health officials in an aggregated, anonymized format. Even though individual users are not identified, these data could reveal general trends about where and when people are congregating and risking the spread of infection. Another attractive alternative is a contact-tracing app that allows device users to opt in and consent to the use of their data, with transparency about how those data will be used, stored and shared. In Israel, 6 days after the initiation of mandatory coronavirus surveillance by the ISA, the Ministry of Health launched a very similar voluntary service, an open-code application that allows citizens to opt in to logging of their mobile-phone locations. This application notifies mobile users shortly after they come close to a person who has tested positive for SARS-CoV-2 (as recorded by health officials) and advises them to self-isolate. Despite the difficulty of determining proximity among phones and, more importantly, the physical barriers (e.g., personal protective equipment, walls and doors) between users that might prevent transmission, which can result in a high false-positive rate, the application became the most-searched item on Google in Israel overnight. Within a week, over a million people (nearly 20% of the adult smartphone users in Israel) had downloaded the application, even though the similar non-voluntary service run by the ISA already existed. Interestingly, nearly one third of the users removed the application shortly after installing it on their device, reflective of a substantial, yet not perfect, participation rate. The next tier of privacy, which prioritizes the maintenance of civil rights, is completely voluntary data submission and completely anonymized data. A considerable limitation of this approach is that such apps can reduce the spread of disease only if many people use them. In addition, voluntary data submission carries a risk of creating a false sense of security for users because areas without reports might still have infected people who can spread the virus.

During a pandemic, especially one involving a disease whose carriers can

be asymptomatic, mobile and highly contagious, traditional methods to minimize contagion might be insufficient, and no pandemic-fighting tools should be overlooked. At the same time, the parameters set out in existing law cannot be ignored—even at times of crisis—and the balance between privacy and pandemic policy is delicate. The short-term data from Israel on the efficacy of a digital surveillance system and the high rate of voluntary participation in disease surveillance suggest that mass digital tracking is feasible. Given the inherent risks to privacy and civil liberties, however, in the long run, policymakers should use this tool with extreme caution and only for a predefined period, adhering to the principles in Box 1. Applying these rules will prioritize transparency and augment the public trust needed to improve cooperation.

The Israeli experience shows that two thirds of the contacts of infected people go unnoticed; many of those are SARS-CoV-2 spreaders and, in specific populations (e.g., close-knit communities), even super-spreaders. When used under strict, preferably civilian, supervision, advanced technologies could make it possible to minimize restrictions, expedite a return to a normal state and reduce the impact on economies, while saving lives. ❐

Moran Amit[1], Heli Kimhi[1], Tarif Bader[2,3], Jacob Chen[4], Elon Glassberg[2,5,6] and Avi Benov[2,6]✉

[1]Department of Head and Neck Surgery, The University of Texas MD Anderson Cancer Center, Houston, TX, USA. [2]Israel Defense Forces, Medical Corps, Tel Hasomer, Ramat Gan, Israel. [3]Department of Military Medicine, Hebrew University, Jerusalem, Israel. [4]Medical Directorate, Ministry of Health, Jerusalem, Israel. [5]The Uniformed Services University of the Health Sciences, Bethesda, Maryland, USA. [6]The Azrieli Faculty of Medicine, Bar-Ilan University, Safed, Israel.
✉*e-mail: avi.benov@gmail.com*

Published online: 26 May 2020
https://doi.org/10.1038/s41591-020-0927-z

References

1. Worldometer. Coronavirus/Israel https://www.worldometers.info/coronavirus/country/israel/ (accessed 9 April 2020).
2. Massaro, E., Kondor, D. & Ratti, C. *Sci. Rep.* **9**, 16911 (2019).
3. Li, Q. et al. *N. Engl. J. Med.* **382**, 1199–1207 (2020).
4. McMichael, T.M. et al. *N. Engl. J. Med.* https://doi.org/10.1056/NEJMoa2005412 (27 March 2020).
5. Knesset Foreign Affairs and Defense Committee. https://main.knesset.gov.il/Activity/committees/ForeignAffairs/Pages/CommitteeAgenda.aspx?tab=3&ItemID=2086830 (2020).
6. Israel supreme court discusses state surveillance against civilians [video]. *YouTube* https://www.youtube.com/watch?v=DQj3SNRYGxw&t=24331s
7. Lis, J. *Haaretz* https://www.haaretz.com/israel-news/.premium-knesset-panel-extends-shin-bet-coronavirus-tracking-by-another-three-weeks-1.8821398 (5 May 2020).
8. Knesset Foreign Affairs and Defense Committee. https://main.knesset.gov.il/Activity/committees/ForeignAffairs/News/Pages/pr_050520.aspx (2020).

Acknowledgements

We thank A. Ninetto of the Department of Scientific Publications at The University of Texas MD Anderson Cancer Center for editing the manuscript.

Competing interests

The authors declare no competing interests.