Comment

SEONGJOON CHO/BLOOMBERG VIA GETTY

Passengers on an underground train in Seoul. South Korea used contact tracing to great effect early in the pandemic.

Ethical guidelines for COVID-19 tracing apps

Jessica Morley, Josh Cowls, Mariarosaria Taddeo & Luciano Floridi

Protect privacy, equality and fairness in digital contact tracing with these key questions.

Technologies to rapidly alert people when they have been in contact with someone carrying the coronavirus SARS-CoV-2 are part of a strategy to bring the pandemic under control. Currently, at least 47 contact-tracing apps are available globally (see go.nature.com/2zc1qhk). They are already in use in Australia, South Korea and Singapore, for instance. And many other governments are testing or considering them.

Here we set out 16 questions to assess whether – and to what extent – a contact-tracing app is ethically justifiable. These questions could assist governments, public-health agencies and providers to develop ethical apps – they have already informed developments in France, Italy and the United Kingdom. They will also help watchdogs and others to scrutinize such technologies.

What do COVID-19 contact-tracing apps do? Running on a mobile phone, they inform people that they have spent time near someone with the virus. The contacts should then respond according to local rules, for example by isolating themselves. Prompt alerts are key because the incubation time of the virus is up to two weeks[1–4].

These digital interventions come at a price. Collecting sensitive personal data potentially threatens privacy, equality and fairness. Even if COVID-19 apps are temporary, rapidly rolling out tracing technologies runs the risk of creating permanent, vulnerable records of people's health, movements and social interactions, over which they have little control.

More ethical oversight is essential. So far, such concerns have focused on rights to privacy (see go.nature.com/3e7jntx). Some governments have pledged to protect data privacy (see go.nature.com/3grwfe8). Apple and Google are developing a common interface to support apps that do not require central data storage (see *Nature* http://doi.org/dwc6;

2020). However, other ethical and social considerations must not be cast aside in the rush to quell the pandemic.

For instance, contact-tracing apps should be available and accessible to anyone, irrespective of the technology needed or their level of digital literacy. Yet many apps work only with certain phones. Australia, for example, has no plans to make its app work with phones that use software older than Apple's iOS 10 or Android 6.0. In the United Kingdom, around one-fifth of adults do not use a smartphone, and so might be excluded from a digital contact-tracing programme.

Rolling out an app without considering its wide ethical and social implications can be dangerous, costly and useless. For example, Bluetooth signals that show the proximity of two individuals' mobile phones are not a certain indicator of infection risk — two people might be in the same space but physically separated, for example, by a wall. A high level of false positives from such an app (for instance, as a result of self-reporting) could lead to unjustified panic. And minimal protections against false negatives (people not using the app to report that they are unwell) could spur a false sense of safety in others and increase the risk of infection.

The public might reject apps that breach principles of privacy, equality and fairness. This would frustrate the efforts and waste the resources being invested in developing and deploying such technology. Lack of consideration of ethics could erode trust in the government and public-health services — as happened last month, when the Norwegian Data Protection Authority accused the Norwegian Institute of Public Health of failing to carry out a proper risk assessment of its contact-tracing app, Smittestopp.

Many approaches

Temporarily restricting some fundamental rights and freedoms might be ethically justifiable in the context of hastening the end of the pandemic. Quarantining individuals, for example, helps to prevent the spread of the disease. Arguably, it might be unethical not to use digital tracing apps when necessary. Nevertheless, much depends on the effectiveness of the app, the goal pursued, the type of system and the context in which it will be deployed.

Countries and regions are taking different approaches. China's Alipay Health Code app assigns a digital QR code to each user, which is colour-coded red, amber or green to indicate that person's quarantine status and thus their ability to move around. People quarantined in Hong Kong must wear an electronic bracelet that shares their location with local authorities through an app. Poland requires citizens to self-isolate for 14 days after returning from overseas, and to

Guidelines

Is this contact-tracing app ethically justifiable?

Those responsible for contact-tracing apps should answer the following.

Principles: is this the right app to develop?

1. Is it necessary?
- Yes, it must be developed to save lives (+).
- No, there are better solutions (–).

2. Is it proportionate?
- Yes, the gravity of the situation justifies the potential negative impact (+).
- No, the potential negative impact is disproportionate to the situation (–).

3. Is it sufficiently effective, timely, popular and accurate?
- Yes, evidence shows that it will work, is timely, will be adopted by enough people and yields accurate data and insights (+).
- No, it does not work well, is available too late or too early, will not be used widely, and is likely to collect data that have false positives and/or false negatives (–).

4. Is it temporary?
- Yes, there is an explicit and reasonable date on which it will cease (+).
- No, it has no defined end date (–).

Requirements: is this app being developed in the right way?

5. Is it voluntary?
- Yes, it is optional to download and install (+).
- No, it is mandatory and people can be penalized for non-compliance (–).

6. Does it require consent?
- Yes, people have complete choice over what data are shared and when, and can change this at any time (+).
- No, default settings are to share everything all the time, and this cannot be altered (–).

7. Are the data kept private and users' anonymity preserved?
- Yes, data are anonymous and held only on the user's phone. Others who have been in contact are notified only that there is a risk of contagion, not from whom or where. Methods such as differential privacy are used to ensure this. Cyber-resilience is high (+).
- No, data are (re)identifiable owing to the level of data collected, and stored centrally. Locations of contacts are also available. Cyber-resilience is low (–).

8. Can users erase the data?
- Yes, they can do so at will; all data are deleted at the end point (+).
- No, there is no provision for data deletion, nor a guarantee that it can ever be deleted (–).

9. Is the purpose of data collection defined?
- Yes, explicitly; for example, to alert users that they have encountered a potentially infected person (+).
- No, the purposes of data collection are not explicitly defined (–).

10. Is the purpose limited?
- Yes, it is used for tracing and tracking of COVID-19 only (+).
- No, it can be regularly updated to add extra features that extend its functionality (–).

11. Is it used only for prevention?
- Yes, it is used only to enable people voluntarily to limit spread (+).
- No, it is also used as a passport to enable people to claim benefits or return to work (–).

12. Is it used for compliance?
- No, it is not used to enforce behaviour (+).
- Yes, non-compliance can result in punishment such as a fine or jail time (–).

13. Is it open-source?
- Yes, the code is publicly available for inspection, sharing and collaborative improvement (+).
- No, the source code is proprietary, and no information about it is provided (–).

14. Is it equally available?
- Yes, it is free and distributed to anyone (+).
- No, it is arbitrarily given only to some (–).

15. Is it equally accessible?
- Yes, it is user-friendly, even for naive users, and works on the widest possible range of mobile phones (+).
- No, it can be used only by those with specific devices and with sufficient digital education (–).

16. Is there a decommissioning process?
- Yes, there is a process for shutting it down (+).
- No, there are no policies in place (–).

send geotagged 'selfies' to the police to prove they are at home. Singapore's TraceTogether app has been downloaded by about 25% of its population, much less than the 60% needed. This has led the country to introduce its SafeEntry system, which requires users to check in to public places using their national identity card or by scanning a QR code with their phone.

Apps differ in how they collect and store data. For example, they might rely on systems that are centralized, as in Australia and Singapore, or decentralized, as in Germany and Italy (see also *Nature* http://doi.org/dwc6; 2020). Centralized apps send pseudonymized data collected by a user's phone to a central database controlled by, for example, a national health agency, where contacts are matched. Decentralized approaches instead match contacts on the user's device (see go.nature.com/3e7jntx). Use of an app can be voluntary, as the European Commission recommended in April (see go.nature.com/2x2hrat), or not. India's app, for instance, is mandatory for citizens living in virus-containment zones and for all government and private-sector employees. Apps in Argentina and the United Kingdom ask users to self-report their symptoms, whereas the Norwegian app relies on the user having a formal diagnostic test.

More coordination is needed. Some supranational efforts to harmonize the apps are under way. The World Health Organization, for example, is developing a symptom-checking app that might also enable contact tracing in under-resourced countries. The European Data Protection Supervisor has called for a Europe-wide contact-tracing app[5]. The European Commission has outlined requirements for digital tracing solutions deployed in the European Union, including compliance with EU data protection and privacy rules[1].

Countries and regions should consider a broader set of ethical concerns, including equality and fairness. Government agencies and developers working under pressure might find it hard to make these judgement calls quickly. In other contexts, such as bioethics, ethical review boards typically have much more time to deliberate. Expert groups might be set up to advise, as France, Italy and the United Kingdom have done. (L.F. is a member of the UK National Health Service COVID-19 App Data Ethics Advisory Board; see go.nature.com/3cxyzrw).

Four principles

To be ethical, a contact-tracing app must abide by four principles: it must be necessary, proportional, scientifically valid and time-bound. These principles are derived from the European Convention on Human Rights, the International Covenant on Civil and Political Rights (ICCPR) and the United Nations Siracusa Principles, which specify the provisions in the ICCPR that limit how it can be applied.

However, there are many ways in which an app can meet these principles. To address this gap, we have synthesized 16 questions that designers, deployers and evaluators should answer (see 'Is this contact-tracing app ethically justifiable?'). For each, we give examples of how an app might be designed and used in a more (+) or less (–) ethically justifiable way. These questions apply to apps that have been released, as well as for those in development[6].

In theory, an ethical app should satisfy all 16 factors. The questions themselves might not be controversial, but the answers are likely to generate disagreement about whether and how much an app satisfies a factor, and which ethical factors should be a priority.

> **"Governments might not have a second chance to get an intervention right."**

In practice, there will be trade-offs. These will depend on the laws, values, attitudes and norms in different regions, as well as on changes over time in the spread and scale of the virus and the available technology. For example, it might be more ethically justifiable to deploy an app that does not fully meet the stipulation that it should "work on the widest possible range of mobile phones" in a country with high smartphone penetration, such as South Korea – where more than 95% of people owned a smartphone in 2018. But it might be less justifiable in Japan, where 66% of the population did.

Similarly, what was ethically justifiable in one place yesterday might not be so tomorrow. For example, Germany shifted from a centralized to a decentralized app after some 300 experts signed an open letter strongly criticizing the centralized approach. The same happened in Italy after Apple and Google announced their plan to support decentralized apps. Singapore could follow suit. Its centralized TraceTogether app was developed before the Apple–Google interface was available, and developers are now aiming to make it compatible.

An app's implementation strategy and impact must also be considered. Something that looked good on paper can turn out to be ineffective in practice. This was the case with the Australian COVIDsafe app. Concerns about third-party access to user data and low compatibility with phones running old operating systems have led to a low level of adoption. More than a month since deployment, the minimum threshold of 40% has not been met. This is making the app irrelevant for managing the pandemic in Australia.

If an app fails, it becomes unnecessary, and thus unethical. Apps that are no longer beneficial should be improved or decommissioned. A review and exit strategy must be in place to establish when and how fast this should happen. These assessments should be conducted by an independent body, such as a regulator or an ethics advisory board, and not by the designers or the government itself. Circumstances and attitudes are changing quickly, so the questions in our framework must be asked anew at regular intervals.

One chance

Governments might not have a second chance to get an intervention right – failure now could breach public trust for the foreseeable future. Governments, developers and deployers must ensure that COVID-19 contact-tracing apps satisfactorily address the ethical questions we set out. Apps that do not should not be deployed; alternatives should be considered.

Simply rolling out a tracing app without ethical consideration is not acceptable. Even in a crisis, a 'try-everything' approach is dangerous when it ignores the real costs, including serious and long-lasting harms to fundamental rights and freedoms, and the opportunity costs of not devoting resources to something else.

The authors

Jessica Morley is a graduate researcher at the Oxford Internet Institute, University of Oxford, UK. **Josh Cowls** is a doctoral researcher at the Oxford Internet Institute, University of Oxford, UK, and at The Alan Turing Institute, London, UK. **Mariarosaria Taddeo** is a senior research fellow at the Oxford Internet Institute, University of Oxford, UK, and a Turing Fellow/DSTL Ethics Fellow at The Alan Turing Institute, London, UK. **Luciano Floridi** is professor of philosophy and ethics of information at the Oxford Internet Institute, University of Oxford, UK, and a Turing Fellow and chair of the Data Ethics Group at The Alan Turing Institute, London, UK.
e-mail: pa.floridi@oii.ox.ac.uk

1. European Commission. *Commission Recommendation (EU) 2020/518 of 8 April 2020* (EC, 2020); available at https://go.nature.com/2jkmmpt
2. European Centre for Disease Prevention and Control. *Novel Coronavirus Disease 2019 (COVID-19) Pandemic: Increased Transmission in the EU/EEA and the UK — Sixth Update* (ECDC, 2020).
3. Ferretti, L. *et al. Science* **368**, eabb6936 (2020).
4. Keeling, M. J., Hollingsworth, T. D. & Read, J. M. Preprint at medRxiv https://doi.org/10.1101/2020.02.14.20023036 (2020).
5. Wiewiórowski, W. *EU Digital Solidarity: A Call for a Pan-European Approach Against the Pandemic* (European Data Protection Supervisor, 2020).
6. Floridi, L. *Phil. Trans. R. Soc. A* **376**, 20180081 (2018).