Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems

Jessica Morley[1*^], Josh Cowls[1,2^], Mariarosaria Taddeo[1,2^], Luciano Floridi[1,2^]

[1] Oxford Internet Institute, University of Oxford, OX1 3JS
[2] The Alan Turing Institute, British Library, 96 Euston Rd, London NW1 2DB

*Correspondence to: jessica.morley@oii.ox.ac.uk
^All authors contributed equally to the writing of this document

Summary

The World Health Organisation declared COVID-19 a global pandemic on 11th March 2020, recognising that the underlying SARS-CoV-2 has caused the greatest global crisis since World War II. In this article, we present a framework to evaluate whether and to what extent the use of digital systems that track and/or trace potentially infected individuals is not only legal but also ethical. Digital tracking and tracing (DTT) systems may severely limit fundamental rights and freedoms, but they ought not to be deployed in a vacuum of guidance, to ensure that they are ethically justifiable, i.e. coherent with society's expectations and values. Interventions must be *necessary* to achieve a specific public health objective, *proportional* to the seriousness of the public health threat, *scientifically sound* to support their effectiveness, and *time-bounded* (1,2). However, this is insufficient. This is why in this article we present a more inclusive framework also comprising twelve enabling factors to guide the design and development of ethical DTT systems.

The Ethical Risks of COVID-19 Digital Tracking and Tracing Systems

The COVID-19 pandemic has necessitated extraordinary interventions in the physical space — where governments are limiting freedom of movement and assembly — and in the digital space, where governments are fostering extensive data collection and analysis to improve their capacity to tackle the pandemic and to support research on the behaviour of the virus. According to the COVID-19 Digital Rights Tracker, as of 20th April 2020 there were 43 contact tracing apps available globally (3,4). These systems may include real-time collection of data related to an individual's location and health status (i.e. symptoms, confirmed infection) and their contact with other individuals. Calls to develop DTT systems continue to grow as the crisis unfolds. In Europe alone, the European Data Protection Supervisor has called for a pan-European tracking app (5); the European Commission has defined a 'toolbox' to support the development of DTT systems (6); protocols like PEPP-PT and DP-3T are being developed at European level (7); Italy is developing a contact-tracing smartphone app (8); and England's NHSX is planning to introduce a comparable app (9,10), possibly based on (10). Meanwhile, Apple and Google are working on a shared solution that includes application programming interfaces (APIs) and operating system-level technology to assist in contact tracing around the world (11).

Since COVID-19 has a relatively long incubation period, a considerable amount of disease spread appears to occur when people are carrying the virus but are not yet symptomatic. Therefore, alerting a user as early as possible when they come into contact with an infectious person and encouraging them to self-isolate could limit the propagation of disease and interrupt transmission chains, potentially hastening the end of the pandemic (6,12–14). In this scenario, the temporary restriction of some fundamental rights and freedoms may be ethically justifiable. Equally it may be unethical *not* to use DTT systems. But this decision requires adequate analysis of the ethical implications of the use of a particular DTT system in a given context. The challenge is that continually shifting circumstances make analysing the ethical implications of different DTT system difficult. The difficulty increases when ethical considerations are presented as superficial and secondary to the

government's urgent need to manage the pandemic. The development of an ethically unjustified DTT system may mean developing a DTT system which would be useless and wasteful, or even dangerous. For it may exacerbate problems like social panic, social shaming, the erosion of trust in the government and public health services, or inequality. Furthermore, it may facilitate potentially unethical uses of personal data originally collected for the purpose of contact tracing that may impact privacy, severely and perhaps irreversibly. This is why it is crucial, even at the time of a global crisis, to consider ethical risks and implement adequate measures to avoid or minimise them.

Guidelines for Ethically Justifiable Design and Development of Digital Tracking and Tracing Systems

The European Convention on Human Rights, the United Nations International Covenant on Civil and Political Rights, and the United Nations Siracusa Principles indicate when and how rights can be restricted to prevent the spread of infectious disease. All three documents stress that measures infringing on fundamental rights must be time-bound, and meet standards of necessity, proportionality and scientific validity. We consider these the foundations of the ethical justifiability of DTT systems. On these foundations we developed a framework comprising 16 questions that can be used to assess whether a given DTT system is ethically justifiable.

The framework (Figure 1) consists of *high-level principles* and *enabling factors*. The high-level principles are those identified in the aforementioned documents: *necessity*, *proportionality*, *scientific soundness*, and *time-boundedness*. These principles are universal and all-encompassing, permitting an answer to the overall question "is the *correct* DTT system being developed?" (what in engineering is known as "validation" of the product). They offer go/no-go criteria. The enabling factors are concrete considerations, derived from the high-level governance principles and digital ethics, with specific pertinence to the COVID-19 public health crisis and proposed uses of DTT systems to tackle it. They enable one to answer the overall question "is the DTT system being developed *correctly*?" (what in engineering is known as "verification" of the product). The enabling factors translate the longstanding, universal high-level principles (the *what*) into practical, ground-level considerations for designers and deployers of DTT systems (the *how*). Note that there is more than one ethical way to design a DTT system. It is also possible for one DTT system to be more or less ethically justifiable than another. This is why, for each of the questions in the framework, there is an illustration of a more (+) or less (-) ethically justifiable answer. There is also a theoretical, and moveable, threshold of justifiability that must be reached. Reaching this threshold depends on a number of more justifiable design decisions as well as on how exactly a more justifiable design is achieved in a given context. Ultimately these decisions are political. This variability is necessary because exactly how to achieve a more ethically justifiable design will depend on the wider context in which the DTT system is being deployed. For example, the same app that may be ethically justifiable in a country with a small and digitally literate population, like Singapore, may not be simply importable as a solution for a country with a much larger population and a more significant digital divide, like the UK. Similarly, what was ethically justifiable in one place yesterday may not be so tomorrow as circumstances and attitudes change. This means that the questions must be iterated regularly.

Questions to determine the extent to which a DTT is ethically justifiable

High-level Principles (answer the question: is the correct DTT system being developed?)

1) Is it a necessary solution?
   + Yes, the app must be developed to save lives.
   - No, better solutions are available.
2) Is it a proportionate solution?
   + Yes, the potential negative impact of the DTT system is justified by the gravity of the situation.
   - No, the potential negative impact of the DTT system is disproportionate to the situation.
3) Is it scientifically sound?
   a) Will it be effective?
      i) Is the timing 'right'?
      ii) Will adoption rates be high enough?
      iii) Will it be accurate?

   + Yes, evidence shows that the system will work, is a timely solution, will be adopted by a sufficient number of people, and yields accurate data and insights.
   - No, the app does not work well, arrives too late or too soon, will not be adopted extensively, and is likely to collect data that are insufficiently accurate (too many false positives and/or false negatives).
4) Is it temporary?
   + Yes, there is an explicit and reasonable sunset clause.
   - No, its deployment has no defined end date.

Enabling Factors (answer the question: is the DTT system developed correctly?)

5) Is it voluntary?
   + Yes, it is optional to download and install the app
   - No, it is unnecessarily mandatory and sanctions may be applied 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, the default data settings of the app 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 completely anonymous, held only on the user's phone. Others found to have been in contact are only notified that there is a case of contact at risk of contagion, not with whom or where the contact took place. Methods such as differential privacy are used to guarantee this. Cyber-resilience is high.
   - No, data are completely (re)identifiable due to level of data collected, and stored centrally. Locations of contacts are also available. Cyber-resilience is low.
8) Can the data be erased by the users?
   + Yes, users can delete data at will, and in any case all data will be deleted at sunset (see 4).
   - No, there is no provision for data deletion or guarantee that it can ever be deleted.
9) Is the purpose defined?
   + Yes, it is clearly defined, the app notifies individuals only when they have been in contact with people with confirmed infection, and only essential data are collected (e.g. confirmed health status and time of contact).
   - No, terms and conditions are loosely defined, there is no guarantee that data will not be used for secondary and only loosely related purposes, data collected may also be combined with other databases. Multiple data sources may be collected, without any transparency, with no user control.
10) Is the purpose limited?
    + Yes, the app is used for personal monitoring purposes only.
    - No, the app can be regularly updated adding extra features that extend its functionality, e.g. for future studies about pandemic risks.
11) Is it used only for prevention?
    + Yes, the app is used only to enable people voluntarily to prevent spread ("flattening the curve").
    - No, the app is also used as a passport, e.g. to enable people to claim benefits or return to work ("support phase two").
12) Is it used to monitor users' behaviour?
    +No, the app is not used to comply with any required behaviour.
    - Yes, the app is used to monitor behaviour
13) Is it open-source?
    + Yes, the source code of the app is made available, so all aspects of design can be inspected, sharing is supported, and collaborative improvements are facilitated.
    - No, the source code of the app is unavailable, and no information about it is provided in any other form.
14) Is it equally available?
    + Yes, the app is freely and widely distributed to anyone who wishes to download it and use it.
    - No, the app is arbitrarily given only to selected users.
15) Is it equally accessible?
    + Yes, the app is freely and widely distributed to anyone who wishes to download and use it.
    - No, only those with specific mobile phones, part of specific digital ecosystems, and with sufficient digital education can use the app.
16) Is there an end-of-life process to retire the system?
    + Yes, there is a clear road map to deal with the app being officially discontinued.
    - No, there are no policies in place to manage the final stage of maturity of the app.

Figure 1: Framework for ascertaining the ethical design and development of DTT systems.

The context-dependency of the ethical justifiability of a DTT system requires considering the whole lifecycle of the system and the progression of the pandemic. For instance, in some circumstances the voluntary nature of the app might become negotiable. Or consider an app that is initially launched as a voluntary download and which requires a 60% adoption rate to be scientifically effective but is only adopted by 20% of the population (e.g., for reasons of poor access or lack of trust). In this case, low adoption-rate may not only undermine the effectiveness but also heighten a false sense of security (it will not be true that "no news is good news") and the risk of identifiability of individuals, damaging privacy and increasing the potential for public shaming. In this instance, the app which may on paper have looked to be ethically justifiable, becomes ineffective, and therefore unnecessarily and disproportionately intrusive. Likewise, an app that falls foul of a cyberattack could become at best ineffective and at worst dangerous. In these circumstances, the only option would be to 'turn off' the system. For all these reasons, there also must be an exit strategy (question 16) in place for when the DTT system is no longer needed, useful, or ethically justifiable, and it must be possible to act on the strategy rapidly, in the case of failure. It follows that a clear deadline *by when* and a clear indication of *by whom* the whole project will be assessed and in case be terminated, improved, or even simply renewed as it is, is essential.

Only One Chance to Get It Right

These are extraordinary times and some extraordinary measures may be required. But the severity of the crisis does not justify using any possible means to overcome it. Fundamental rights and freedoms still need to be protected in both the physical and digital space, and guidance is urgently needed on how to ensure this protection.

We have argued that a DTT system that satisfies the four principles of necessity, proportionality, scientific soundness and time-boundedness is ethically justifiable depending on the extent to which it satisfies 12 additional factors. Even if the methodology, justification for and theoretical approach of a DTT system is valid, if circumstances make it impossible to verify its design (by addressing the 12 factors sufficiently), then it should not be used. This is because, when choosing between deploying or not deploying a DDT system we are not facing a win-win situation where, if a DTT system works it is to be lauded, and if it does not, then no harm is considered to have occurred. Governments planning to deploy DTT despite poor design and limited verification of their ethical justification may be doing so to demonstrate a willingness to "try everything", and hence avoid blame. This is dangerous even, or indeed especially, in a time of crisis, because it treats all costs, including harms to fundamental rights and freedoms, that an ethically wrong DTT solution may bring as externalities (they affect the future, the next government etc.). In the case of COVID-19, the costs (all kinds of them) are high and ought not to be dismissed as "externalities": they will hit the current population and its governments deeply and quickly, potentially making the whole problem worse, because the ethically wrong kind of DTT system is not merely ineffective, it may exacerbate the problem it seeks to solve. Governments only have one chance to get an intervention right, as repeated failures and overly high costs breach citizens' trust. Ethical analysis sheds light on risks and opportunities, and offers a compass with which to align urgent decision-making with the longstanding values that underpin societies, and with societal expectations regarding the appropriate scope of governance. This is why treading ethically in time of crisis is crucial to success.

References

1. EDPB. Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak [Internet]. 2020 [cited 2020 Mar 30]. Available from: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

2. Ada Lovelace Institute. COVID-19 Rapid Evidence Review: Exit through the App Store? [Internet]. 2020 Apr [cited 2020 Apr 20]. Available from: https://www.adalovelaceinstitute.org/our-work/covid-19/covid-19-exit-through-the-app-store/

3. Top10vpn. Covid Digital Rights Tracker [Internet]. Available from: https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/

4. Knight W. Phones Could Track the Spread of Covid-19. Is It a Good Idea? 2020 Mar 15; Available from: https://www.wired.com/story/phones-track-spread-covid19-good-idea/

5. Wiewiórowski W. EU Digital Solidarity: a call for a pan-European approach against the pandemic Wojciech Wiewiórowski [Internet]. 2020 [cited 2020 Apr 20]. Available from: https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf

6. European Commission. COMMISSION RECOMMENDATION of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. Brussels; 2020 Apr.

7. Troncoso C, Payer M, Hubaux J-P, Salanthe M, Larus J, Bugnion E, et al. Decentralized Privacy-Preserving Proximity Tracing [Internet]. 2020 Apr [cited 2020 Apr 12]. Available from: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

8. Pollina E, Goodman D. Italy Tests Contact-Tracing App to Speed Lockdown Exit. New York Times [Internet]. 2020 Apr 17 [cited 2020 Apr 20]; Available from: https://www.nytimes.com/reuters/2020/04/17/technology/17reuters-health-coronavirus-italy-technology.html

9. Downey A. NHSX working on coronavirus contact tracking app. Digital Health [Internet]. 2020 Mar 20 [cited 2020 Mar 30]; Available from: https://www.digitalhealth.net/2020/03/nhsx-coronavirus-contact-tracking-app/

10. Keilon L. Coronavirus: UK confirms plan for its own contact tracing app. BBC News [Internet]. 2020 Apr 12 [cited 2020 Apr 16]; Available from: https://www.bbc.co.uk/news/technology-52263244

11. Keyword team. Apple and Google partner on COVID-19 contact tracing technology [Internet]. Google. 2020 [cited 2020 Apr 11]. Available from: https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/amp/

12. ECDC. Novel Coronavirus disease 2019 (COVID-19) pandemic: increased transmission in the EU/EEA and the UK - sixth update [Internet]. 2020 Mar [cited 2020 Mar 30]. Available from: https://www.ecdc.europa.eu/sites/default/files/documents/RRA-sixth-update-Outbreak-of-novel-coronavirus-disease-2019-COVID-19.pdf

13. Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science [Internet]. 2020 Mar 31 [cited 2020 Apr 6];eabb6936. Available from: https://www.sciencemag.org/lookup/doi/10.1126/science.abb6936

14. Keeling MJ, Hollingsworth TD, Read JM. The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19). [Internet]. Public and Global Health; 2020 Feb [cited 2020 Mar 27]. Available from: http://medrxiv.org/lookup/doi/10.1101/2020.02.14.20023036