

Covid-19 contact tracing: efficacy and privacy

Aengus Collins
May 2020

This article assesses the risk-risk trade-off between privacy and efficacy that the use of contact-tracing apps entails. It concludes that app-based approaches enjoy important advantages for tracing Covid-19 and that privacy risks can be mitigated. However, it notes a number of digital-tracing weaknesses and cautions that current debates about tracing should not detract attention from other pillars of the Covid-19 response, such as testing.

More and more countries are beginning to attempt to unwind at least some of the restrictions that have been imposed over recent months to suppress outbreaks of Covid-19. The effort to return to more normal societal conditions will entail numerous novel policy challenges, most of which are going to have to be resolved in conditions of significant ongoing uncertainty. In the first of our articles in this Spotlight series, we used elements of the IRGC risk governance framework to consider the broad sweep of the Covid-19 outbreak and countries' responses to it.¹ This article uses a risk lens to analyse one specific policy dilemma with which policy-makers are now grappling: the use of smartphone technology to contribute to the process of contact tracing.² This is a novel possibility – this is the first smartphone pandemic – and it raises immediate privacy concerns. In risk governance terms, this is an instance of a risk-risk trade-off, where a policy intervention made with a view to mitigating one risk may cause or exacerbate another risk.³

In the context of Covid-19 there is a potential trade-off between app-based contact tracing's efficacy (its contribution to halting the spread of the disease) and app users' privacy (the risk that tracing apps will lead to the collection and misuse of personal data).⁴ The exact parameters of this trade-off are not yet clear, but the risk lens helps to home in on salient aspects and balance between different objectives. In practice, developers and privacy specialists have been able to demonstrate that robustly privacy-preserving contact tracing is possible. In other words, the societal benefits of digital tracing can be captured without any loss of privacy. The key example of this work is the DP-3T protocol, which has been developed by an international team including colleagues here at EPFL, and which is being used as the basis for apps being developed by a range of countries, particularly in Europe.⁵ DP-3T has also been acknowledged as an influence on the joint solution that Apple and Google have been working on and that is likely to have a significant bearing on the kind of apps that can be successfully deployed.⁶ However, the implementation of privacy-preserving solutions does not mean that the privacy-efficacy trade-off has been resolved: there are aspects of digital tracing, and privacy-preservation more specifically, that may be less effective than more traditional tracing methods. As we will see, one example is the inability of privacy-preserving apps to give healthcare workers the details needed to contact at-risk individuals directly.

It is important to note at the outset that in practice the trade-off between privacy and efficacy will operate differently in different countries, depending on cultural, political and societal differences. In a country with high levels of trust in the public authorities, weaker privacy preservation may not reduce the support for digital tracing. Conversely, in a low-trust country uptake of a tracing app may be low even if there are assurances that strong privacy-preservation protocols are being adhered to.

How contact tracing works

Comparing the functioning of app-based contact tracing and human contact tracing is a useful way of illustrating potential strengths and weaknesses of both. However, it is important to note that here is no need to make a policy choice between the two. They can operate simultaneously and in practice this is what is happening in many countries in

response to Covid-19.⁷ Traditionally, contact tracing involves public health workers interviewing infected individuals to identify the people they have been in contact with, so that follow-up interventions can be made and appropriate healthcare measures can be advised or imposed.⁸ This is a labour-intensive process, and one which has typically been used for sexually transmitted diseases and other infections that spread more slowly than Covid-19.⁹ It also raises privacy concerns: it is designed to create contact lists of named individuals with whom health workers can follow up.¹⁰ These privacy risks need to be mitigated, but they are not of the same magnitude as the potential risks of digital tracing which could establish surveillance tools that would be easy to misuse.

A privacy-preserving tracing protocol like DP-3T is designed not to rely on any identifying data. Instead it uses the proximity of phones as a proxy for the risk of infection spreading between the phones' users. Under the decentralised DP-3T protocol, smartphones generate anonymous and frequently changing "ephemeral identifiers" and broadcast them on an ongoing basis using Bluetooth. No location data is recorded or shared. Other smartphones that encounter these ephemeral identifiers store them, along with a record of the duration of the encounter. If a user subsequently tests positive for Covid-19, she can instruct the app to upload her identifiers to a central server. Other apps periodically cross-reference their stored identifiers against the list of infected identifiers on the server. If there is a match, then the app assesses whether the proximity and duration of the encounter pose a high risk of infection (using parameters set by the health authority). If the encounter is assessed as high risk, the app informs the at-risk user and typically suggests what the next steps are. For example, in Switzerland the user is told to contact the health authorities using a hotline number. The notification that the app provides is anonymous. It does not identify the infected user and does not specify the time or location of the encounter that triggered the notification. In addition, at no point are any of the users identified by the app to the public health authorities or to any other entity. It is only when the at-risk individual voluntarily contacts the hotline that the process stops being anonymous, with the individual taken through an interview by a health worker and provided with appropriate medical advice.

Potential efficacy gains

What about the efficacy of such privacy-preserving digital approaches to contact tracing? There are at least two ways in which any app-based tracing may be more effective than traditional contact tracing. The first of these relates to **speed and scale**. Contact tracing needs to outpace the spread of a virus in order to stifle an outbreak: there is a “race to trace”.¹¹ As transmissibility increases – and Covid-19 is highly transmissible – human tracing becomes less effective. There is an inverse relationship between the efficiency of human contact tracing and the reproductive rate of a disease.¹² This constraint does not apply to app-based tracing: there is no loss of efficiency as the number of encounters increases or as greater numbers of at-risk notifications are required.¹³ This also points to an important point about cost. One advantage of digital tracing is that it can be scaled up instantly using technology that many people already carry around with them. To scale up human tracing involves recruitment programmes potentially requiring extensive time and investment.¹⁴

A second advantage of digital tracing is that unlike human tracing it does not rely on people’s memories to capture encounters that may pose a risk of infection. The **high number of encounters recorded** may lead to false positives,¹⁵ but it allows the capture of many potentially significant encounters – for example on public transport – that a person being interviewed may not be able to recall.¹⁶ This is particularly important in the case of Covid-19 given the extent of asymptomatic transmission. A related advantage is that digital tracing allows the health authority to specify the proximity and duration parameters that should trigger the notification process. This is not without technical challenges, but again it compares favourably with human tracing’s reliance on individuals’ memories, which are likely to be hazy as to the proximity and duration of many encounters.

Potential weaknesses of digital tracing

Against these potential efficacy gains, there are four potential weaknesses to be considered. Two relate to digital tracing in general, while the others concern privacy-preserving apps more specifically. The first of the general issues is that these apps cannot be launched in isolation: they need to be

connected to the rest of the public health system. The technology used by contact tracing apps is relatively straightforward, but **integration with existing healthcare systems and processes** can be a major challenge, depending on factors such as the level of centralisation or decentralisation across the health system, or the existing technology platforms which the health system uses and with which a new app may need to communicate.

The second general issue is that the efficacy of these apps is tied to the number of people using them. For a proximity-tracing system to register an encounter, both individuals must have the app installed. At low levels of **uptake across the population**, this becomes a drag on efficacy. For example, if 60% of the population has installed the app, then on average 36% of encounters will be traced. If installation drops to 30%, then just 9% of encounters will be traced. It is also possible that installation rates will be lower in certain groups that are more vulnerable to Covid-19, such as elderly people. The lower the level of uptake, the less effective an app will be. It is true that even at lower levels of uptake, app-based tracing will continue to contribute to pushing down the reproduction rate of the virus, and also that digital tracing will be deployed alongside rather than instead of human tracing. But at very low levels of uptake, the contribution of digital tracing may be minimal. Singapore for example was one of the first countries to begin digital tracing, but uptake of its TraceTogether app stood at just 17% ten days after launch. This means that on average just 3% of encounters could be traced.¹⁷ Another early app, Stopp Corona in Austria, has reportedly been downloaded by only 7% of the population.¹⁸ At a time when some policymakers risk hyping what app-based tracing is likely to accomplish,¹⁹ it is important to be upfront about these potential limitations with a view to ensuring a balanced policy debate across the range of interventions that are needed in response to Covid-19. The current focus on digital tracing should not divert attention away from other crucial elements of this phase of the pandemic response, such as testing.²⁰

It is also important to note that privacy may boost uptake and efficacy. Subject to the caveats in the introduction about background levels of trust in a society, being able to demonstrate that privacy is protected may be an important factor in encouraging users to install a tracing app. The same is true of a robust governance framework, which may include authorising legislation, although

what is viewed as sufficiently robust may differ significantly across countries. In the UK, Lilian Edwards and others have produced draft contact-tracing legislation which includes safeguards such as a requirement that all data collected is deleted at the end of the emergency (or earlier), the creation of a dedicated oversight commission, and the right of all individuals to initiate legal proceedings if they feel their rights under the legislation have been breached.²¹ Insights from behavioural science will also have an important bearing on optimising the uptake of tracing apps – for example by helping to structure individual incentives to participate.²²

Potential weaknesses of privacy-preserving tracing

As mentioned above, there are two potential weaknesses that arise when privacy-preservation is added to digital tracing. Another way of looking at these is as societal benefits that might be lost by insisting on privacy-preservation. The first of these issues relates to **epidemiological data**. A number of epidemiologists, particularly in the UK, have said that strict privacy-preservation hampers the collection of data that could be used to understand the virus better.²³ The DP-3T protocol allows users to consent to sharing as much epidemiological data as is possible while preserving privacy. Typically, this means data relating to the timing of infections: when in the infectious period are contacts between infected and at-risk users being recorded?²⁴ Of course, these are not the only epidemiologically relevant data, particularly with a new disease like Covid-19 about which so much remains uncertain. There is an epidemiological cost to not being able to distinguish whether or how transmission varies for different age groups, for example, or between men and women. Or in other words, there is a potential societal benefit from using non-privacy-preserving technologies because they allow for more epidemiological data collection. However, the collection of this richer data does not need to take place within the contact tracing app. The objective of the app is to find at-risk individuals and prompt them to contact the health authorities – as soon as contact is made, richer data about the individual can be collected by the healthcare worker in the course of a standard interview. As noted above, uptake is crucial to the efficacy of digital contact tracing and privacy-preservation may be one way of boosting uptake. Removing privacy-preservation to capture more epidemiological data risks weakening uptake

in order to complete a task that can be handled elsewhere.

The second potential privacy-preserving weakness concerns the nature of the **notification process** when a high-risk encounter has been flagged. As discussed above, under a privacy-preserving approach like DP-3T, the user receives an app notification requesting, for example, that they make contact with the health authority. There is no compulsion to make contact, and there is no way of following up in person with potentially infected people who do not voluntarily contact the health authority. With human tracing, by contrast, it is the public health worker who initiates contact with potentially infected contacts. This is also the case in a non-privacy-preserving digital tracing system like Singapore's TraceTogether, mentioned above. With TraceTogether, users cannot identify each other, but once an infection is notified, public bodies are able to identify and follow up with any individuals who are flagged as having been in high-risk proximity with the infected user.²⁵ It is an empirical question whether it makes a significant difference to the effectiveness of the Covid-19 tracing process whether a potentially infected user receives an anonymous app notification or is contacted directly by a health worker.²⁶ In general, we might expect an in-person call to be more effective than electronic messages from an app.²⁷ However, this is not clearly the case. For example, human contact tracing in Massachusetts has run into difficulties because at-risk individuals are not responding to phone calls from the public health authorities.²⁸ This suggests that we need to distinguish not just between digital and human contact tracing, but also between human tracing conducted via telephone and human tracing conducted much more labour-intensively by knocking on doors.

Any firm conclusions on the most effective form of notification must await the emergence of data as apps are deployed, as human contact tracers do their work, and as more is learned about how people respond to both digital and human tracing.²⁹ In principle, though, it is possible that anonymous app-based notifications could be less effective compared to apps that provide health workers with the information to initiate contact with at-risk individuals.

Conclusion

This article has sought to highlight salient features of the potential trade-off between privacy and efficacy that arises with the advent of digital contact tracing as pandemic response tool. On the privacy side of the trade-off, the article pointed to the DP-3T protocol as evidence that privacy concerns can be mitigated with the use of privacy-preserving technologies. On efficacy, the picture is mixed. We noted two important ways in which digital tracing may be more effective than human tracing: its capacity to operate at a speed and scale that match a disease like Covid-19, and its ability to capture close contacts that human tracing might miss. But we also highlighted four potential weaknesses, two of which, in particular, may turn out to limit efficacy significantly: the level of uptake across the population, and reliance on app-based notifications to encourage at-risk users to contact the public health system.

Neither of these potential weaknesses is sufficient to warrant non-deployment of digital tracing – conclusions should be drawn as evidence becomes available. However, these weaknesses are sufficient to call for caution about the extent of the contribution of digital tracing to the pandemic response. Digital tracing apps have become the focus of intense international attention, to the possible detriment of the wider policy debate. The limitations of digital tracing should be acknowledged clearly, and it should be emphasised that tracing is just one of a number of key responses (notably including testing) that will be required simultaneously as countries unwind their Covid-19 restrictions.

Acknowledgements

The author would like to thank the following individuals for their insightful comments while this article was being drafted: Gérard Escher (EPFL), Marie-Valentine Florin (IRGC@EPFL), Jim Larus (EPFL), Kenneth Oye (MIT), Janos Pasztor (Carnegie Climate Governance Initiative), Ortwin Renn (Institute for Advanced Sustainability Studies).

- ¹ Aengus Collins, “Covid-19: a risk governance perspective,” 2020. [↗](#)
- ² For a brief overview of a range of digital contact tracing apps, see Johns Hopkins Center for Health Security, “Review of mobile application technology to enhance contact tracing capacity for Covid-19,” April 8, 2020. [↗](#)
- ³ John D. Graham, Jonathan Baert Wiener, and Cass R. Sunstein, *Risk vs. Risk* (Harvard University Press, 1995).
- ⁴ In the EU, the General Data Protection Regulation (GDPR) makes specific provision for the use of personal data in the context of a public health emergency. However, any such use is still subject to “data minimisation” and “purpose limitation” requirements.
- ⁵ Carmel Troncoso et al., “Decentralized privacy-preserving proximity tracing: overview of data protection and security,” April 3, 2020. [↗](#)
- ⁶ Apple – Google, “Exposure notification: FAQ,” 2020. [↗](#)
- ⁷ For an early estimate of the relative effectiveness of digital and human contact tracing, see Adam J Kucharski et al., “Effectiveness of isolation, testing, contact tracing and physical distancing on reducing transmission of SARS-CoV-2 in different settings,” preprint (Epidemiology, April 29, 2020). [↗](#)
- ⁸ For a detailed discussion of human contact tracing for Covid-19 in the US, see Crystal Watson et al., “A national plan to enable comprehensive Covid-19 case finding and contact tracing in the US” (Johns Hopkins Center for Health Security, 2020).
- ⁹ Matt J Keeling, T. Deirdre Hollingsworth, and Jonathan M Read, “The efficacy of contact tracing for the containment of the 2019 novel coronavirus (Covid-19),” preprint (Public and Global Health, February 17, 2020). [↗](#)
- ¹⁰ World Health Organisation, “Contact tracing,” May 9, 2017. [↗](#)
- ¹¹ Edward H. Kaplan, David L. Craft, and Lawrence M. Wein, “Emergency response to a smallpox attack: the case for mass vaccination,” *Proceedings of the National Academy of Sciences* 99, no. 16 (2002): 10935–10940.
- ¹² K. T. D. Eames and M. J. Keeling, “Contact tracing and disease control,” *Proceedings of the Royal Society of London. Series B: Biological Sciences* 270, no. 1533 (December 22, 2003): 2565–71. [↗](#)
- ¹³ Another important consideration for tracing at scale relates to cases involving individuals who have crossed borders. The decentralised approach of DP-3T allows cross-border tracing without the exchange of identifying data: the user’s phone cross-references its stored ephemeral identifiers with the lists of infected identifiers on the backend servers of any countries the user has been visiting.
- ¹⁴ Watson et al., “A national plan to enable comprehensive Covid-19 case finding and contact tracing in the US.”
- ¹⁵ Ada Lovelace Institute, “Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the Covid-19 crisis,” 2020, 26. [↗](#)
- ¹⁶ Marcel Salathé and Ciro Cattuto, “Covid-19 response: what data is necessary for digital proximity tracing?” GitHub, April 9, 2020. [↗](#)
- ¹⁷ Clara Chong, “About one million people have downloaded TraceTogether app,” *The Straits Times*, April 1, 2020. [↗](#)
- ¹⁸ Douglas Busvine, “European coalition takes shape on coronavirus contact tracing,” Reuters, May 7, 2020. [↗](#)
- ¹⁹ Gaby Hinsliff, “Even if it works, this coronavirus tracking app is no get-out-of-jail-free card,” *The Guardian*, May 5, 2020, sec. Opinion. [↗](#)
- ²⁰ For a proposal on how to combine digital contact tracing with “smart testing”, see Hossein Gorji et al., “STeCC: smart testing with contact counting enhances Covid-19 mitigation by Bluetooth app based contact tracing,” *MedRxiv*, May 7, 2020. [↗](#)
- ²¹ Lilian Edwards et al., “The coronavirus (safeguards) bill 2020: proposed protections for digital interventions and in relation to immunity certificates,” 2020.

- ²² Stefan Volk, “Coronavirus contact-tracing apps: most of us won’t cooperate unless everyone does,” *The Conversation*, April 22, 2020. [↗](#)
- ²³ Helen Warrell, Tim Bradshaw, and Sarah Neville, “UK starts to build second contact tracing app,” *Financial Times*, May 8, 2020. [↗](#)
- ²⁴ Troncoso et al., “Decentralized privacy-preserving proximity tracing: overview of data protection and security,” 5.
- ²⁵ Hyunghoon Cho, Daphne Ippolito, and Yun William Yu, “Contact tracing mobile apps for Covid-19: privacy considerations and related trade-offs,” *ArXiv:2003.11511 [Cs]*, March 30, 2020. [↗](#)
- ²⁶ Andrea Renda, “Covid-19 and privacy: a European dilemma,” *Trigger*, April 8, 2020. [↗](#)
- ²⁷ Susan Holtzman et al., “Emotional support during times of stress: can text messaging compete with in-person interactions?” *Computers in Human Behavior* 71 (June 1, 2017): 130–39. [↗](#)
- ²⁸ Boston Herald, “Answer the call by talking with MA COVID Team,” *Boston Herald*, May 10, 2020. [↗](#)
- ²⁹ For reporting of what contact tracing involves in practice, see Caroline Haskins et al., “We need an ‘army’ of contact tracers to safely reopen the country. We might get apps instead,” *BuzzFeed News*, accessed May 3, 2020. [↗](#)