HHS Public Access

Author manuscript

Am J Bioeth. Author manuscript; available in PMC 2020 November 11.

Published in final edited form as:

Am J Bioeth. 2020 July ; 20(7): W7–W11. doi:10.1080/15265161.2020.1764136.

The Value and Ethics of Using Technology to Contain the COVID-19 Epidemic

Alex Dubov[a], **Steven Shoptaw**[b]

[a]University School of Behavioral Health, Loma Linda, CA

[b]UCLA, Los Angeles, CA, USA

INTRODUCTION

As the world grapples with COVID-19, experts are calling for better identification and isolation of new cases. In this paper, we argue that these tasks can be scaled up with the use of technology. Digital contact tracing can accelerate identifying newly diagnosed patients, instantly informing past contacts about their risk of infection, and supporting social distancing efforts. Geolocation data can be used to enforce quarantine measures. Social media data can be used to predict outbreak clusters and trace the spread of misinformation online. These technology tools have played a role in turning the tide of the epidemic and easing lockdown measures in China, South Korea, and Singapore. There is a growing interest in the US in digital contact-tracing tools that may help rein in contagion and relax lockdown measures. This paper provides an overview of the ways in which technology can support non-pharmaceutical interventions during the COVID-19 epidemic and outlines the ethical challenges associated with these approaches.

CONTACT TRACING

According to recent findings (Hellewell et al. 2020), about 70% of contacts need to be traced to control the majority of outbreaks. Additionally, a study suggests that 86% of COVID-19 cases are undocumented (pre-symptomatic), and these cases are responsible for 55% of all documented cases (Li et al. 2020). Given the high rates of infection and the significant contribution to transmission from asymptomatic individuals, the traditional efforts to halt the epidemic by contact tracing and isolation are simply not possible. The alternative approach of widespread quarantine measures and lockdowns are also unlikely to be sustained for long periods, especially in open societies. Technology can scale up traditional epidemiological methods and offer a way to relax restrictive lockdown without sacrificing the protection of citizens. Rapid identification and isolation of cases and exposures, made possible by mobile geolocation or Bluetooth data, is a promising way to reduce contact rate. We will review successful examples of digital contact-tracing in various countries and discuss the ethical implications of using these methods.

China is relaxing the lockdown measures by asking citizens to use the Alipay Health Code app. After reporting their travel history and current symptoms, Health Code users receive a color-based QR-code indicating their health status. Users with a red code are instructed to be quarantined for 14 days; users with a yellow code are told to stay inside for 7 days, while

users with a green code may travel freely. The app is used to track movement at travel checkpoints (train stations or highways) as well as at the neighborhood level. All services require people to show their QR-codes before entering. Over 700 million people are using Health Code (Tencent Official Website). *Israel* will be tracking individuals' phones to find out where a suspected carrier has been and with whom they have come into contact. Potential contacts will be notified through text messages with orders to self-quarantine. These orders can be further enforced through the location-tracking capabilities of cellphones (Halbfinger 2020). In *Taiwan*, people who are ordered to self-quarantine are monitored using a mobile-phone based location-tracking 'electronic fence.' The system monitors phone signals to alert officials if quarantined patients move away from their address or turn off their phones. Officials also call twice a day to ensure people don't avoid tracking by leaving their phones at home (Wang et al. 2020). On March 20, *Singapore* released the *TraceTogether* app that uses Bluetooth to track when two app users have been in close proximity. The app exchanges time-limited tokens between nearby phones. These tokens are also sent to a central server. When a person reports they have been diagnosed with COVID-19, the app allows the Ministry of Health to determine anyone who logged to be near them. A human contact tracer will alert these contacts and determine appropriate follow up actions.

Similar approaches are currently considered by other governments, including the UK and the US. A team of medical researchers at Oxford University encourage the UK government to explore the use of mobile apps for instant contact tracing. If rapidly and widely deployed, they believe such an app could help to contain the spread of COVID-19 (Ferretti 2020). MIT researchers released a prototype of an app (Private Kit: Safe Paths) that uses geolocation to warn people about their exposure risks (Raskar 2020). The MIT approach will be further adapted by eight European countries participating in Pan-European Privacy-Preserving Proximity Tracing project (PEPP-PT Official Website). The project proposes to create an open-source app that analyzes Bluetooth signals between phones to detect users who are close enough to infect each other. The WHO is considering a similar app for digital contact-tracing to be promoted worldwide (Strickland 2020).

A global contact-tracing tool can be a product of the recent collaboration between Google and Apple. The two tech giants have joined forces to develop an opt-in contact-tracing tool, similar to the Singaporean *TraceTogether* app (Kupferschmidt 2020). Both companies will make changes to their operating systems to let devices exchange a private key with nearby phones via Bluetooth, logging any time users come in close proximity. If someone tests positive for COVID-19 and enters that information into an app, 14 days worth of their contacts with other users are sent to a server. These contacts will be advised to take precautionary measures. This tool will not collect location or personally identifiable data and will not identify people who test positive to other users.

The future success of a digital contact-tracing tracing tool is directly proportionate to its uptake by the public. However, in the first ten days of TraceTogether roll-out, only one million people (or one in six Singaporeans) have downloaded it (TraceTogether Official Website). Experts are skeptical about levels of adoption for a similar digital contact-tracing tool in societies like the US or UK. A recent Pew Research Center study provided some

evidence of public acceptance of digital surveillance tools. 52% of respondents said it is at least somewhat acceptable for the government to use people's phones to track the location of those who have tested positive for COVID-19. At the same time, 45% of the public said it is acceptable for the government to use phones to track the location of people who may have had contact with a virus carrier. Only 37% of surveyed people believed it is appropriate for the government to use phones to track compliance with social distancing measures (Anderson and Auxier 2020).

In addition to digital contact-tracing, data mining on social media can provide insights into the timing and geography of the coronavirus spread in the US, as it has been previously used for tracking seasonal flu on Twitter (Achrekar 2011). Finally, at-home devices such as wearables or mass-distributed smart thermometers that store results automatically on the cloud, can be used for early case identification. For instance, Kinsa Health, the company that has previously used internet-connected thermometers to predict the spread of flu, now tracks the coronavirus in real-time (Chamberlain 2020). Hong Kong and Bahrain are using electronic tracker wristbands to geofence people under quarantine (Wong et al. 2020).

Using technology for early case identification on the population level presents multiple ethical challenges.

1. Testing. For digital contact-tracing to work, there needs to be enough COVID-19 tests for anyone who believes they're positive. Contact-tracing apps rely on users to report if they were tested positive. The apps, then, can use Bluetooth to find all the other phones that were in contact with the virus carrier and notify them. Cryptography ensures that the apps cannot identify individuals on either end. Users should not be able to report that they are COVID-19 positive without an independent verification (test results). Therefore, the wide availability of COVID-19 testing is a crucial component for these apps to work. According to the COVID Tracking Project, the number of tests performed in the US has plateaued at about 130,000 to 160,000 a day (The COVID Tracking Project 2020). Several analysts suggest that the US should be conducting a minimum of 500,000 tests a day to keep the epidemic in check (Morgan Stanley Research 2020). The ability to access testing should not be linked to the use of digital contact-tracing.

2. Aggregated vs. identifiable data. There are several ways in which population mobility data can be collected: (1) anonymized location pings that map mobile density to understand compliance with social distancing; (2) tracking location and movements of devices anonymized into broad patterns and providing estimates of aggregate flows of people; (3) privacy-sensitive location tracking on an individual level relying on users to share their location history when they test positive. Users that came close to that phone receive notification of their risk of infection and are advised to self-isolate. Location data is stored on individual phones and is only shared with third-party users when users test positive. Notifications about the risk of infection are de-identified; (4) government-led efforts that trace individual movements and release information on those who test positive. Anonymous aggregated data can be shared with governments and

researchers within the constraints of existing laws and regulations. However, some app and device-makers can be sued for sharing data in a way that wasn't specified in their terms of service, unless specific legislation would free them from liability. Several countries (Germany and UK) are in the process of designing such legislation. On March 19, the European Data Protection Board adopted a statement allowing the Member States to introduce legislative measures to safeguard public security, at the same time permitting them to use non-anonymized data with adequate safeguards (The European Data Protection Board 2020). Measures aiming to override consent and privacy rights in the name of surveillance may fuel distrust, especially in places where citizens have a lower level of trust in their governments. An ethical alternative is a third-party contact-tracing app freely downloaded by users who give their consent to location tracing and disclosure of information in a privacy-sensitive manner. Any use of location tracing should come with safeguards to ensure the data is not retained or used for any other purposes than epidemic containment. Access and use of data should be limited and highly regulated, and any abuse of these terms should be followed by harsh penalties.

3. Voluntary consent. Consent-based data sharing is the most ethical approach to data sharing for contact tracing as a way to mitigate privacy risks. However, there might be several issues in implementing consent procedures such as language barriers, lack of comprehension, and absence of choice. Typically, to benefit from using a contact-tracing app (e.g. exposure risk assessment), users need to either share their location with a third party or enable their Bluetooth settings. It is plausible that diagnosed users may lack the option to deny consent. This possibility should be avoided as no one should be obligated to share their personal information, even under conditions of public health emergencies. Given that digital contact-tracing will only be successful when enough people participate, any compulsory measure will be resisted. Therefore, voluntariness needs to be preserved on each step of digital contact-tracing implementation—decisions to carry a smartphone, decisions to download contact-tracing app, decisions to leave this app operating at the background, decisions to react to its alerts, and decisions to share contact logs when testing positive for COVID-19.

4. Privacy risks. Digital contact-tracing comes with several privacy risks. Carriers of COVID 19 are at the most significant risk as they can be identified even by a limited set of location data needed to alert their potential contacts. Users of contact-tracing apps may face similar risks by allowing third-parties to access their location. Local businesses can be impacted when they are identified as places visited by a COVID 19 carrier and ordered to close. Maximum effort should be undertaken to protect the privacy of diagnosed people. Publicly available data should be limited to protect identities. Users should consent to sharing their location data, and the involvement of third-party entities in the data sharing process should be limited or eliminated. Whenever possible, collected data should stay local to participants' devices and, if the system uses identifiers, they should not be linked to other identifiable information.

5. Transparency in implementation, including a transparent/auditable algorithm. Decisions about the implementation of mobile contact tracing should be made in a transparent way that encourages input from all stakeholders. For instance, transparency around people's classification by Health Code was lacking, and, as a result, people were afraid and bewildered when they were ordered to isolate themselves without knowing the reasons. Public officials need to disclose their reasons for implementing a contact-tracing intervention and safeguards built into this intervention. Algorithms that will operationalize any case identification intervention should be open to public scrutiny to ensure fairness, accuracy, and absence of bias. Similarly, an app should be developed using an open-source approach, enabling independent experts and media to access and evaluate the source code.

6. Data security. There is a need for multiple protections against data loss and unauthorized access. The unauthorized access may include employers or health insurance companies. Effective database management, including encryption and automated backup procedures, needs to be implemented. One way to maintain privacy and data security at the same time is to allow data to be encrypted and stored on users' phones. This information is only shared upon request or when users test positive (Cho et al. 2020). Storing only anonymized and aggregated data, and limiting data storage to the time when a person can be contagious is another way to protect data security.

7. Governance. Given numerous historical examples of abuse of vulnerable individuals in the name of the public good, officials planning to implement a mobile case identification need to assemble a diverse advisory board to provide oversight. Civil liberties advocates and various public voices need to be involved in determining data uses, collection, and resulting interventions. Already existing government advisory boards such as the Health Care Industry Cybersecurity Task Force can function as an oversight body for digital contact-tracing. One of the critical tasks of this governing body would be to provide updates on the impact of digital contact-tracing (e.g. number of app installations, number of self-isolations, or contacts with health professionals). These updates will further promote the adoption of contact-tracing tools by giving people a sense of whether these tools are effective. The governing body should also identify measures to phase out digital contact tracing due to low numbers of new infections or a lack of effective impact on the epidemic.

8. Assurance of equitable access to treatment and absence of stigma. Asian Americans and people returning from cruise ships have already been subjected to pandemic-related harassment in the US (Lin 2020). It is essential to guide the implementation of contact tracing approaches in a way that reduces stigma. Efforts to curb the epidemic should not turn people's mobile phones into a digital version of the medieval leper bell. Technological solutions often tend to exacerbate exciting stigmas—e.g. hiring algorithms worsen gender disparities and criminal justice algorithms aggravate racial biases. Digital contact-tracing should be applied sensibly and in a non-punitive way. For instance, instead of

local authorities enforcing isolation, these tools might allow health professionals to alert quarantine-breakers of the risk. Additionally, access to treatment should not be conditioned on the use of the app or data gleaned from the app.

9. Opt-in vs. opt-out enrollment. Several nations that implemented mobile case identification approaches have chosen various implementation strategies. In China, the enrollment was voluntary, but the system was set up in such a way that participation was essential to perform daily functions. In Israel, the recipients of governmental notifications had not signed up for the tracking system, and they couldn't opt-out. In Singapore, participation was voluntary, with a moderate level of uptake from citizens. States planning to adopt digital contact-tracing need to consider opt-in enrollment that would preserve individual autonomy.

10. Efforts to include vulnerable groups and populations. Uptake of a mobile app will be limited among the most vulnerable groups—elderly, homeless, and economically disadvantaged. Additionally, 21.6% of the US population are non-English speakers (Mizoguchi 2019) and about 10 million (Fazel-Zarandi et al. 2018) are undocumented immigrants. The mobile intervention may not reach vulnerable groups, if they have no access to mobile phones, or if they cannot navigate an app interface due to language or tech literacy, or if they are worried about the security of their private data. Efforts to implement digital contact-tracing should go hand in hand with determining which groups are likely to be excluded or misrepresented by these tools. Additional funding needs to be directed to support these groups. These tools should not be used to further marginalize these groups—e.g. using them for criminal prosecution or immigration enforcement. Even with limited access, contact-tracing technology will increase the safety of the population as a whole. Access to information about possible contagion can be made available even to those who lack phones and presented in an easy to understand language.

CONCLUSION

There is a need for an ethical framework for digital epidemiology and technological interventions to support contact tracing in public health emergencies. The successful use of these interventions can only be achieved if they can secure public trust. This paper aimed to outline several requirements for these interventions to be ethical and to be able to ensure public confidence during the COVID-19 pandemic such as privacy-preserving design; voluntariness in uptake; avoidance of discrimination and punishment resulting from the use of the app; open-source approach; maintenance by a governing body; data destruction protocols and use limitations; reliable data security protocols preventing a third party from accessing data; minimal collection of data that is stored locally.

There is an urgent need for continued open and informed discussion about the ethical implications, quality, and safety of technology-driven interventions during epidemics. Questions for discussion might include:

1. Given the public benefits (timeliness, accuracy) of using mobile data for disease surveillance, should the use of identifiable data be permitted, and in what circumstances? Do individuals have a moral obligation to share this data? Should individual consent be required and under what circumstances?
2. What level of probability and reliability, based on data gleaned from individual mobile data, should be required before requiring preventative measures? How much explanation do we owe the public about these measures and reasons behind them?
3. What level of transparency and what degree of oversight is needed for these interventions to gain public trust and acceptance? What steps need to be implemented to prevent stigmatization of certain population groups? What are the most effective ways to avoid the misuse of the data? What should be done with the collected data and mobile apps when the epidemic is over?
4. What level of incentives should be implemented for the population to participate in mobile contact-tracing? What degree of quarantine enforcement is ethically appropriate when live geolocation data is available to health officials?
5. To what degree should predictive algorithms be trusted for early identification and facilitation of preventative methods? What are the best practices to ensure the transparency of algorithms and their applications?
6. Though mobile technology is increasingly widespread and available, access is not uniform. What measures should public health officials implement to ensure fairness in access and proper representation?
7. How should we protect the privacy of data and minimize access to personal sensitive information for implementing mobile contact-tracing? What is the appropriate balance of individual privacy against public safety?

Acknowledgments

FUNDING

This work was supported by National Institute of Mental Health. Grant Number P30MH058107

REFERENCES

Achrekar H, Gandhe A, Lazarus R, et al. 2011 Predicting flu trends using twitter data. 2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS) IEEE.

Anderson M, and Auxier B. 2020 Most Americans don't think cellphone tracking will help limit COVID-19, are divided on whether its acceptable. https://www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable/ (accessed April 16, 2020)

Chamberlain SD, Singh I, Ariza CA, et al. 2020 Real-time detection of COVID-19 epicenters within the United States using a network of smart thermometers. medRxiv.

Cho H, Ippolito D, and Yu YW. 2020 Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs. arXiv 2003: 11511.

The COVID tracking project. 2020 Covidtracking.com/.

The European Data Protection Board. 2020 Statement on the processing of personal data in the context of the COVID-19 outbreak. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

Fazel-Zarandi MM, Feinstein JS, and Kaplan EH. 2018 The number of undocumented immigrants in the United States: Estimates based on demographic modeling with data from 1990 to 2016. PLOS One 13(9): e0201193. [PubMed: 30240392]

Ferretti L, Wymant C, Kendall M, et al. 2020 Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science. doi: 10.1126/science.abb6936.

Halbfinger D, Kershner I, and Bergman R. 2020 To track coronavirus, Israel moves to tap secret trove of cellphone data. NY Times. https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html.

Hellewell JS Abbott A Gimma NI, et al. 2020 Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. The Lancet Global Health 8(4): E488–E496. [PubMed: 32119825]

Kupferschmidt K 2020 The lockdown worked – but what comes next? Science 368(6488): 218–219. [PubMed: 32299926]

Li R, Pei S, Chen B, et al. 2020 Substantial undocumented infection facilitates the rapid dissemination of novel coronavirus (SARS-CoV2). Science.

Lin C-Y 2020 Social reaction toward the 2019 novel coronavirus (COVID-19). Social Health and Behavior 3(1): 1.

Mizoguchi N, Walker L, Trevelyan E, and Ahmed B. 2019 The older foreign-born population in the United States: 2012–2016. United States Census Bureau. https://www.census.gov/content/dam/Census/library/publications/2019/acs/acs-42.pdf.

Morgan Stanley Research. 2020 COVID-19: A prescription to get the US back to work.” https://www.dcba-pa.org/UserFiles/files/events/Biotechnology_%20COVID-19_%20A%20Prescription%20To%20Get%20The%20US%20Back%20To%20Work.pdf.

Pan-European privacy-preserving proximity tracing project. https://www.pepp-pt.org/

Raskar R, Schunemann I, Barbar R, et al. 2020 Apps gone rogue: Maintaining personal privacy in an epidemic. arXiv 2003: 08567.

Strickland E 2020 An official WHO coronavirus app will be a ‘waze for COVID-19. IEEE Spectrum. https://spectrum.ieee.org/the-human-os/biomedical/devices/who-official-coronavirus-app-waze-covid19.

Tencent official website. https://mp.weixin.qq.com/s/J6tp773LtabcQGeUy36ixA.

TraceTogether official website. https://www.tracetogether.gov.sg/.

Wang CJ, Ng CY, and Brook RH. 2020 Response to COVID-19 in Taiwan: Big data analytics, new technology, and proactive testing. JAMA 323(14): 1341–1342. [PubMed: 32125371]

Wong SYS, On KK, and Chan FKL. 2020 What can countries learn from Hong Kong's response to the COVID-19 pandemic? CMAJ. Available at: https://www.cmaj.ca/content/early/2020/04/24/cmaj.200563