Covid-19 and Contact Tracing Apps: Technological Fix or Social Experiment?

Federica Lucivero 1*, Nina Hallowell 1 †, Stephanie Johnson 1†, Barbara Prainsack 2,3†,

Gabrielle Samuel 3†, Tamar Sharon 4†.

Affiliations:

1 Ethox and Wellcome Centre for Ethics and Humanities, Nuffield Department of Population

Health, Big Data Institute, University of Oxford.

2 University of Vienna.

3 King's College London.

4 iHub, Radboud University.

*Correspondence to: federica.lucivero@ethox.ox.ac.uk

† The authors' names are in alphabetical orders and they equally contributed to the article.

Abstract

Mobile applications are increasingly regarded as important tools for an integrated strategy of post-lockdown policy response around the globe. This paper explores how the use of smartphone applications for digital contact tracing is currently being framed by media, experts and policy-makers and discusses a number of questions raised by the debate on digital surveillance at the time of Covid-19: How can personal data be adequately collected and protected? Who should access data? What is a legitimate role for Big Tech companies in the development and implementation of these systems? How is the cultural and moral context taken into account in the design of these apps? Should use of these apps be compulsory? What does transparency and ethical oversight mean in this context? As we show that responses to these questions are complex and uncertain, we argue that rather than technological fixes to the current emergency these apps should be introduced in society as societal experimental trials whose effectiveness and consequences need to be closely and independently monitored the same level of precaution and safeguards that social experimentation require.

Introduction

The Alipay Health Code App was developed by Ant Financial, a sister company of Alibaba and initially deployed in Hangzhou, China during the COVID-19 outbreak. The Health Code algorithm matches actively collected data (self-reported symptoms, individual's address, personal ID) and passively collected data such as GPS location, and assigns the individual a coloured code (Green, Amber, Red) which, when combined with

scanned QR codes, determines access to public areas, such as subways, malls and markets (Mozur, Zhong, and Krolik 2020). A similar app, originally used during the MERS epidemics, has been deployed in South Korea. Another app "Trace Together" has been launched by the Singapore government as tool to support and supplement manual contact tracing thanks to the Bluetooth technology. As reported by national newspapers and government agencies, other countries, such as Israel, Norway and Iceland have started using similar warning, symptom detection, risk calculation and contact tracing apps since the beginning of the outbreak. As we write, a modelling study by Oxford academics and NHSX supporting the adoption of intelligent contact-tracing has recently been published (Ferretti et al. 2020) and the European Commission has recommended a pan-European approach to the adoption of tracking apps by outlining principles as well as practical measures for inter-state and inter-agency collaborations (European Commission 2020).

There is widespread agreement that digital surveillance may be an efficient way to save lives when exiting national lockdowns in the current COVID-19 crisis. At the same time, there is increasing concern that the temporary restrictions that digital surveillance entails, namely on privacy, data protection and freedom of movement, could lead to a more permanent suspension of rights and liberties. This paper explores crucial questions that should inform decision-making and early phases of implementation of contact tracing applications for smartphones to help contain the spread of this pandemic.

Surveillance and public health

Patient data is routinely collected and curated for the purpose of disease surveillance, for example, in cancer and notifiable disease registries. Typically, traditional epidemiological surveillance has been based on data collected by public health agencies through health personnel in hospitals, doctors' offices, and out in the field (Salathé, 2012). More recently, novel data sources have emerged where data are collected directly from individuals through the digital traces they leave (Eysenbach, 2009). Data from search engines can now provide early warning of respiratory illnesses in local communities, data from social networking sites can provide early warning of vaccine refusal, and tracking population movements with mobile phone network data has improved response to disasters and outbreaks (Bengtsson, 2011). One of the key advantages of digital surveillance, apart from the increasingly large data volumes, is that they are highly contextual and networked (Salathe, 2011). This allows study of individuals and groups in the rich contexts, and the study of person-to-person spread of disease and behaviours that may influence spread (Salathé, 2012). These advantages also raise important questions about the extent of the legitimacy of such highly individual and contextualised surveillance methods in emergency situations.

In the context of infectious disease control, contact-tracing has traditionally been an important means of disease control, involving identifying infected individuals and

informing the people they have been in contact with that they are at risk, through a meticulous process of retracing where and with whom an infected individual has been in proximity. Automated contact-tracing offers several advantages over traditional contact-tracing in the case of the Covid-19 pandemic. First, it seeks to automate a labour-intense practice in a situation where there is a scarcity of human contact tracers. Moreover, it may offer more accuracy where human memories are fallible -- particularly in the case of Covid-19, where infection can be asymptomatic for up to two weeks (Kimball, 2020). At the same time, it raises question about the possibility of trusting algorithms with crucial public health decisions with critical consequences on individuals.

To better understand digital contact tracing apps, we need to contextualise them in ongoing trends in digital data use and automation of public health practices. At the same time, we need to deal with important questions that have been raised about the extent of the legitimacy of such highly granular surveillance methods and automated mechanisms, as well as the fear that if implemented in an emergency an situation, may remain with us for a long time (Harari 2020). Despite the urgency of decision-making in public health emergencies, a rigorous ongoing evaluation of the legitimacy of crisis measures is paramount (Nuffield Council of Bioethics 2020). In the following, we highlight questions that are crucial to address in order to justify a legitimate and ethical use of these apps.

Which safeguards are designed into the technology?

Technologies can be designed in such a way that values, ethical norms and legal principles are built in (Hildebrandt and Tielemans 2013). As such, design decisions can act as powerful limitations for possible excesses in times of crisis, and getting the technical design of contact-tracing apps right is key. Whether these apps will collect geolocation data or Bluetooth signals, whether the data will be stored locally on users' devices or exported to centralized databases run by governments or health authorities, whether these data can also be used for research, whether users have any control over who can access their data and whether data are automatically deleted once the pandemic is over: these are all decisions that translate ethical and legal concerns including consent, purpose limitation, data minimization and data protection into technical design. They require careful deliberation that includes the expertise and voices not just of technology developers, but also privacy and human rights advocates, ethicists and affected groups. A number of European authorities and privacy advocacy groups have emphasized in particular the need for contact-tracing apps to be voluntary, transparent, based on non-traceable identifiers, and de-centralized (Troncoso and et al 2020). Importantly, such design restrictions will never be sufficient on their own, and need to be coupled with institutional, legal and organizational measures.

Who accesses the data?

While in South Korea, data on the movement of individuals were made publicly available on a government website, in other countries, it is often less clear which authorities and other institutions had access to the data. Recent opinion issued by the Information Commissioner's Office in the United Kingdom suggests that use of mobile phone geolocation data for tracking individuals' movement at the spread of contagion is allowable under Data Protection regulations in this public health emergency[1]. Moreover, while it is legally permissible to use health data for public health purposes under the GDPR, ethical questions remain about the nature of these purposes. For example, should law enforcement, in addition to public health authorities, have access to tracking and other health data, and what types of powers should police or other authorities be given to ensure enforcement of lock-down measures?

What should the role of Big Tech be?

In response to the crisis, large tech companies such as Alphabet, Microsoft, Apple, Facebook and Palantir in the West, and Alibaba and Baidu in China, have been invited to contribute to strategies for mitigation in various ways. These include the development of disease surveillance tools, the setting up of testing sites, the use of AI for diagnostics and the funding of Covid-19 related research. In a rare collaboration, Apple and Google have also developed their own version of contact-tracing technology. Importantly, privacy protection is one of the aims of the Apple-Google proposal, which adheres to many of the safeguards required by leading privacy experts, and which may be more privacy-friendly than what some governments, who are pushing for centralized contact-tracing, want ((Kelion 2020)). But while the technical expertise and financial resources that these companies bring to the table may be welcome contributions in times of a global public health crisis, we should be wary of the costs these contributions carry for society further down the line – even if they do safeguard privacy (Sharon 2018; Prainsack 2020). Namely, what kind of dependencies are created on these actors, who are already so powerful in other domains, and to what extent are they taking over functions of public sector actors in the provision of public services? Here too, careful deliberation about the long-term trade-offs involved in immediate mitigation strategies is required.

Efficacy and use: enough evidence?

Questions remain regarding how digital surveillance apps designed for pandemic containment will work in practice. This is because app efficacy is premised on a set of assumptions about human behaviour - assumptions which relate to the fact that a

[1] See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/statement-in-response-to-the-use-of-mobile-phone-tracking-data-to-help-during-the-coronavirus-crisis/

sufficiently large number of people will download the app and use it appropriately. If this assumption proves untrue, then the predictions and inferences about the effectiveness of the app will prove incorrect. Although convincing governmental advice and a coherent media and public health campaign could help to promote uptake and proper use of the app in terms of, for example, adhering to the app's recommendations to self-isolate or respect social distancing when requested, a lack of transparency and concerns about privacy infringement and surveillance could result in a public backlash (Sterckx et al. 2016).

Compulsory or voluntary?

Lack of compliance with lockdown measures in some countries has required stricter enforcement using criminal and pecuniary measures. Despite this, it is suggested that the use of tracking apps should be an individual choice[2].This more libertarian approach to the adoption of tracking apps is not straightforward. First, we can ask to what extent the responsibility for a public health matter should be placed on individuals and what this means in terms of accountability? Furthermore, as one can imagine that in some countries, as in China, individuals could be required to use contact tracing apps if they wished to participate in certain activities (e.g enter public/private spaces) or use public transport (Parker et al. 2020).These restrictions would make the app *de facto* compulsory if individuals are to remain functioning members of society, and would result in discrimination against those who either refuse to use it or do not have smartphones. It could be argued that making the use of tracking apps compulsory is more transparent, and therefore, may be more morally acceptable, than an in-principle voluntary (but *de facto* constraining) approach. However, advocating compulsory adoption to overcome the problem of free riders and avoid *de facto* restrictions cannot overcome the fact that certain groups within society may not be able to access this technology and therefore, if apps are needed to access to certain activities, compulsory adoption will result in the creation of a group of people whose freedoms are curtailed.

Transparency, oversight and accountability

At the time of writing, these questions are currently dividing commentators on the acceptability of contact tracing apps, while decision-makers are keeping silent. But especially when crises require exceptional measures that impact on individuals' liberty, transparency is crucial to maintain legitimacy as it is a means to accountability. In the case of contract tracing apps**,** citizens deserve clarity about many aspects of their

[2] As emphasized by Germany's Justice Minister Christine Lambrecht (https://www.reuters.com/article/us-health-coronavirus-germany-app/german-minister-says-tracking-apps-to-tackle-coronavirus-must-be-voluntary-idUSKBN21I0KM).

implementation: the purpose of data collection, the types of data collected, the parties who have access to them, the extent, modalities and timeline for data deletion, the algorithms and data training sets that will automate processes and influence their daily lives. At present only technical experts are involved in their oversight and assessment[3], through governance mechanisms that are often unclear. Given their potential to threaten privacy and individual liberty, robust oversight of the deployment of these surveillance technologies, which involves users and civil society groups, is urgently needed. Finally, the uncertainties, difficulties and knowledge gaps related to these apps should also be disclosed. It is problematic for politicians or policy makers to portray contact tracing apps as an easy solution to ease our way out of lockdown. Conditions of respect for people's privacy, protection of their data, limiting surveillance to the minimum necessary to overcome the current crisis, as well as conditions for the involvement of powerful private actors in this crisis that adhere to values of democratic governance, need to be rigorously met for national governments to approve of their use.

After these conditions are met, it seems legitimate to treat and evaluate these apps for what they are: one of the many experimental solutions proposed to manage this pandemic. Acknowledging the experimental nature of these technologies means we need to follow a more cautious approach to their adoption and be prepared to monitor and independently evaluate their efficacy and utility. This would mean ensuring that, like other experiments (e.g. clinical trials), there are oversight mechanisms in place which: monitor the societal consequences of the use of apps (for example, the creation of social inequalities through digital exclusion), protect citizens who volunteer to participate in this experiment, and outline clear mechanisms for accountability (delineating who is legally responsible if something goes wrong). This means that we need to develop a transparent organisational and governance infrastructure around these apps. Finally, if all these things are put in place and it appears that these apps do not work as expected, or their harmful side-effects outweigh the promised benefits, then their use must be challenged and eventually terminated.

[3] In Italy, for example, a multidisciplinary task-force of 74 experts have been appointed to evaluate the over 300 proposals of tracking apps that have been submitted to the government https://innovazione.gov.it/nasce-la-task-force-italiana-per-l-utilizzo-dei-dati-contro-l-emergenza-covid-19/.

References

Bengtsson L, Lu X, Thorson A, Garfield R, von Schreeb J. Improved response to disasters and outbreaks by tracking population movements with mobile phone network data: a post-earthquake geospatial study in Haiti. PLoS medicine. 2011;8(8):e1001083.

Eysenbach G. Infodemiology and infoveillance: framework for an emerging set of public health informatics methods to analyze search, communication and publication behavior on the Internet. Journal of medical Internet research. 2009;11(1):e11.

European Commission. 2020. "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." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518&from=EN.

Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing." *Science*, March, eabb6936. https://doi.org/10.1126/science.abb6936.

Harari, Yuval Noah. 2020. "The World after Coronavirus | Free to Read | Financial Times." *Financial Times*, March 20, 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

Hildebrandt, Mireille, and Laura Tielemans. 2013. "Data Protection by Design and Technology Neutral Law." In *Computer Law and Security Review*, 29:509–21. Elsevier Advanced Technology. https://doi.org/10.1016/j.clsr.2013.07.004.

Kelion, K. 2020. "Coronavirus: Apple and France in Stand-off over Contact-Tracing App." *BBC*, April 2020. https://www.bbc.com/news/technology-52366129.

Kimball A HK, Arons M, James A, et al. Asymptomatic and Presymptomatic SARS-CoV-2 Infections in Residents of a Long-Term Care Skilled Nursing Facility — King County, Washington. MMWR. 2020;69(13):377-81.

Mozur, Paul, Raymond Zhong, and Aaron Krolik. 2020. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags - The New York Times." *The New York Times*, March 1, 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

Nuffield Council of Bioethics. 2020. "Ethical Considerations in Responding to the COVID-19 Pandemic." https://www.nuffieldbioethics.org/assets/pdfs/Ethical-considerations-in-responding-to-the-COVID-19-pandemic.pdf.

Parker, Michael, Chrsitophe Fraser, Lucie Abeler-Dorner, and David Bonsall. 2020. “The Ethics of Instantaneous Contract Tracing Using Mobile Phone Apps in the Control of Pandemics.Pdf at Master · BDI-Pathogens/Covid-19_instant_tracing · GitHub.” https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/The ethics of instantaneous contract tracing using mobile phone apps in the control of pandemics.pdf.

Prainsack, Barbara. 2020. “The Political Economy of Digital Data: Introduction to the Special Issue.” *Policy Studies*. https://doi.org/10.1080/01442872.2020.1723519.

Salathe M, Khandelwal S. Assessing vaccination sentiments with online social media: implications for infectious disease dynamics and control. PLoS computational biology. 2011;7(10):e1002199.Salathé M, Bengtsson L, Bodnar TJ, Brewer DD, Brownstein JS, Buckee C, et al. Digital epidemiology. PLoS computational biology. 2012;8(7):e1002616

Sharon, Tamar. 2018. “When Digital Health Meets Digital Capitalism, How Many Common Goods Are at Stake?” *Big Data and Society*.https://doi.org/10.1177/2053951718819032.

Sterckx, Sigrid, Vojin Rakic, Julian Cockbain, and Pascal Borry. 2016. “‘You Hoped We Would Sleep Walk into Accepting the Collection of Our Data’: Controversies Surrounding the UK Care.Data Scheme and Their Wider Relevance for Biomedical Research.” *Medicine, Health Care and Philosophy* 19 (2): 177–90. https://doi.org/10.1007/s11019-015-9661-6.

Troncoso, Carmela, and et al. 2020. “Decentralized Privacy-Preserving Proximity Tracing.” https://github.com/DP-3T/documents/blob/master/DP3T White Paper.pdf.