Duty to Participate in COVID-19 Proximity Tracing

Rethinking Privacy-Health Tradeoffs in a Pandemic

Jiyeon Kim and Neil Richards
Cordell Institute, Washington University in St. Louis

As the COVID-19 pandemic continues to grow, various public health measures are being deployed to slow the spread of the virus. Among those, contact tracing—identifying the contacts of infected individuals to quarantine them—is a critical tool that can reduce the number of transmissions while minimizing the burden on the larger population.[1] While delays in manual contact tracing can render the intervention ineffective, digital contact tracing reduces the delay between case confirmation and identification-notification of contacts and thereby results in effective control of the disease.[2] Digital contact tracing methods can largely be classified into three categories, depending on the type of technology and/or data that is collected. First, requiring to scan a QR code whenever one enters a venue[3]; second, collecting cell phone-based geolocation data complemented by other data such as credit card history[4]; and, third, proximity tracing by Bluetooth signals such as Singapore's TraceTogether app[5] or Apple-Google's application programming interface (API) (also referred to as the "Exposure Notification System").[6]

Countries such as South Korea and China have used either one or both of the first two methods to successfully control COVID-19; however, these countries have also been criticized for concerns of potential privacy invasion particularly involving the use of location data.[7] The Bluetooth-based method, on the other hand, does not collect location data or other personal information.[8] The European Union (EU) Commission has published guidance recommending

---

[1] *See* Joel Hellewell et al. *Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts*, 8 LANCET GLOBAL HEALTH e488 (2020).

[2] *See e.g.*, Luca Feretti et al. *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*, 368 SCIENCE 619 (2020) (demonstrating that instant digital contact tracing can successfully control COVID-19 using a mathematical model); Yasheng Huang, Meicen Sun, and Yuze Sui, *How digital contact tracing slowed COVID-19 in East Asia*, HARV. BUS. REV. (Apr. 15, 2020), https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia (describing how East Asian countries such as China, Korea, Singapore, and Taiwan that used digital contact tracing methods have been successful in controlling COVID-19).

[3] Xinmei Shen, *Shanghai Introduces QR Codes on Subway to Track Potential Contact with Coronavirus*, SOUTH CHINA MORNING POST (Feb. 28, 2020), https://www.scmp.com/abacus/news-bites/article/3052880/shanghai-introduces-qr-codes-subway-track-potential-contact.

[4] South Korea's Infectious Disease Control and Prevention Act, Article 76-2(1)4 authorizes collection of cellphone-based location data, credit card data, and public transportation use data to deterimine the location history of infected patients.

[5] TraceTogether, GovTech, https://www.tracetogether.gov.sg/

[6] Andy Greenberg, *How Apple and Google are enabling COVID-19 contact-tracing*, WIRED (Apr. 10, 2020), https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/.

[7] *See e.g.*, Raymong Zhong, *China's virus apps may outlast the outbreak, stirring privacy fears*, NYTIMES (May 26, 2020), https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html; Kim Arin, *S. Korea walks a fine line between coronavirus tracing, privacy breach*, The Korea Herald (Jun. 9, 2020), http://www.koreaherald.com/view.php?ud=20200609000957.

[8] It has been reported that Google's Android phones require GPS to be enabled for Bluetooth signals thereby raising concerns that location data can be collected while the user is using the Bluetooth-based proximity tracing. Apple

Bluetooth-based proximity tracing,[9] and several European nations have developed apps based on the Apple-Google API. Proximity tracing, however, requires enough uptake within the population in order to be effective,[10] and, by itself, might not be enough as it cannot identify routes of environmental transmission such as contaminated surfaces or environments.

In the US, COVID-19 case numbers are still rapidly rising while the country lacks a coherent contact tracing strategy. It remains largely reliant on traditional manual contact tracing, and only several states are participating in Apple-Google's proximity tracing system.[11] Meanwhile, the Congress has introduced four bills addressing data privacy in digital contact tracing.[12] Despite some differences, the bills share common provisions when it comes to restricting the collection and use of data and ensuring data security. While most provisions are necessary, especially given that there is no federal data privacy law in the US, there is one flaw—requiring "affirmative express consent" for enrollment in digital contact tracing.[13] This stems from an individualistic conception of privacy without considering the nature of public health. In fact, much of the discourse in this pandemic has framed public health measures as "privacy-health tradeoffs"[14] thereby creating unnecessary barriers to implementing effective COVID-19 control strategies even when the privacy risk itself is unclear.

Instead, we argue that a decentralized form of proximity tracing should be mandatory and does not necessarily compromise privacy. First, in decentralized proximity tracing there is no personally identifiable information because the infected individual only provides an anonymized ID to the central database.[15] In addition, there is no centralized form of "proximity data" as contact matching is done on each phone rather than through the central database. Therefore, there is no discernable data privacy risk. Second, because there is no real personal information that is being collected and the risk of re-identification is almost nonexistent, there is no clear reason to

---

phones do not require GPS to be on. Natasha Singer, *Google promises privacy with virus app but can still collect location data*, NYTIMES (July 20, 2020), https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html.

[9] European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01)

[10] Stephanie Findlay, Stefania Palma, and Richard Milne, *Coronavirus contact-tracing apps struggle to make an impact*, FIN. TIMES (May 18, 2020), https://www.ft.com/content/21e438a6-32f2-43b9-b843-61b819a427aa; recently, Apple and Google have announced that their future operating systems will include the Exposure Notification System rather than requiring a separate app, in hopes of increasing participation. *See* Kif Leswing, *Apple and Google will build their coronavirus contact tracing software right into your phone*, CNBC (Sept. 1, 2020), https://www.cnbc.com/2020/09/01/apple-google-will-build-coronavirus-contact-tracing-software-right-into-your-phone.html.

[11] Zac Hall, *Which U.S. states are using Apple's Exposure Notification API for COVID-19 contact tracing?* 9TO5MAC (Aug. 24, 2020), https://9to5mac.com/2020/08/24/covid-19-exposure-notification-api-states/.

[12] COVID-19 Consumer Data Protection Act of 2020 (CCDPA), S. 3663, 116th Cong. (2020); Public Health Emergency Privacy Act (PHEPA), S. 3749 and H.R. 6866, 116th Cong. (2020); Exposure Notification Privacy Act (ENPA), S. 3861, 116th Cong. (2020).

[13] S. 3663, 116th Cong. § 3(a) (2020); S. 3749 and H.R. 6866, 116th Cong. § 3(d)(1) (2020); S. 3861, 116th Cong. § 4(a) (2020).

[14] In fact, privacy is often described to be in conflict with other values. *See e.g.*, COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 23 (MIT 2006) ("The [dominant] privacy paradigm, based on the conceptualization of distinct private and public realms, almost inevitably leads the debate to a discussion of how privacy conflicts with social or community values.")

[15] For a detailed technological description, *see* DP-3T Project, *Decentralized privacy-preserving proximity tracing* (May 25, 2020), https://arxiv.org/pdf/2005.12273.pdf.

require individual consent.[16] In fact, we already require a duty to participate in the Census that collects aggregated data,[17] and arguments have advanced a duty to share electronic health records (EHR) data under certain conditions.[18] Importantly, the Census and healthcare data are all used to further public good where individuals might benefit from other's participation in a rather abstract or indirect manner; in the case of proximity tracing, the condition of reciprocity is more readily met with a more concrete benefit of lower risk of contracting COVID-19, while the grounds for objection to participating are rather weak.[19] While both individualism and solidarity are important tenets of our society, the COVID-19 pandemic provides a case for the importance of solidarity in social crises because only the participation by the majority (or all) of us will enable proximity tracing to work effectively.

Ideally, to maximize the effect of contact tracing, we believe that proximity tracing must be complemented by infected patients' location data to identify potential sources of environmental transmission. Phone-based geolocation data history of infected individuals should be made accessible to public health authorities with strict limitations and safeguards regarding the length of storage, access, use, and security as well as clear rules regarding broadcasting of the location.[20] In fact, infectious diseases are considered as exceptions in many contexts; for example, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule permits disclosure of protected health information regarding "communicable diseases" to public health authorities without consent or authorization.[21] However, collecting location data should be approached carefully given the risk of data misuse and potential for stigmatization and thus requires further investigation into more effective and necessary safeguards.

Rather than facing an undesirable choice of privacy *or* health, we believe that we can achieve both health *and* privacy by properly embracing technology when necessary and promoting the value of solidarity in a pandemic. To a certain degree, privacy is a creature of society and time[22]– perhaps it is time to re-conceptualize privacy for the age of pandemic to ensure a healthier and truly privacy-enhanced future.

[16] Of course, it is necessary to provide clear notice and information about the process.
[17] Alan Wertheimer, *(Why) should we require consent to participation in research?* 1 J. L. BIOSCI. 137, 144 (2014).
[18] I. Glenn Cohen, *Is there a duty to share healthcare data?, in* 209 BIG DATA, HEALTH LAW, AND BIOETHICS (I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena, Urs Gasser eds., 2018).
[19] Professor Cohen provides strong arguments against objections to not imposing a consent requirement for sharing EHR data which are applicable to here as well. *Id.* at 217-19.
[20] South Korea already collects phone-based geolocation data, credit card data, public transportation use data with strict restrictions and conditions under Infectious Disease Control and Prevention Act, Article 76-2. We do not have to collect such wide range of data but can consider adopting the data privacy and security measures when collection location data.
[21] P.L. No. 104-191, 110 Stat. 1938, §164.512(b)(1)(iv) (1996).
[22] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1129-43 (2002).