

POLICY FORUM

PUBLIC HEALTH

Digital exposure tools: Design for privacy, efficacy, and equity

Apps can cut transmission of SARS-CoV-2—but how do we ensure that they don't exacerbate public health inequities?

By Susan Landau^{1,2}

Use of smartphone-based digital contact-tracing apps has shown promise in responding to the COVID-19 pandemic. But such apps can reveal very personal information; thus, their use raises important societal questions, not just during the current pandemic but as we learn and prepare for other inevitable outbreaks ahead. Can privacy-protective versions of such apps work? Are they efficacious? Because the apps influence who is notified of exposure and who gets tested—and possibly treated—we need to consider the apps in the context of health care equity. Exposure-notification apps are predicated on the assumption that if someone is informed of exposure, they will follow instructions to isolate. Such an expectation fails to take into account that isolation—and sometimes even seeking care when ill—is much harder for some populations than others. If apps are to work for all, and not make this worse for disadvantaged populations, there needs to be basic social infrastructure that supports testing, contact tracing, and isolation.

When severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) reached Singapore in spring 2020, the nation instituted a centralized contact-tracing app in which identifiers linked to the user were shared with nearby phones running the app. If a person was diagnosed with SARS-CoV-2, the collected identifiers would be communicated to the Ministry of Health, which would use them to do contact tracing (*1*). Such proximity information—who is near whom for how long—is very revelatory. It can expose a journalist's source or the existence of an extramarital affair. Singapore had originally committed to the data being used solely for tracking

SARS-CoV-2 exposures, but in January 2021, the government changed its policy, permitting the use of app data in criminal investigations.

Researchers and epidemiologists in Europe, the United States, and Australia developed privacy-protective decentralized apps in which contact information remains on the user's phone even while they can learn of their own exposure. Google and Apple, whose phones run the underlying technology, developed engineering infrastructure for such exposure-notification apps with a focus on privacy. By June 2020, the Google-Apple Exposure Notification (GAEN) infrastructure was available, and SwissCovid, the app from Switzerland's Federal Office of Public Health, was rolled out. Other European apps soon followed.

These exposure-notification apps exchange Bluetooth identifiers when two app users are in close proximity for at least 15 min (the apps also handle more sophisticated situations involving exposure by multiple people for shorter periods of time). To protect privacy, the identifiers are randomized strings that change every 10 to 20 min. If one of the app users later tests positive for SARS-CoV-2, they inform public health and then upload the identifiers the phone sent out during their contagious period. They do not share the identifiers they collected; those remain on their phone. All apps check a public health server at predetermined intervals daily and download newly posted identifiers. If one of these identifiers matches an identifier previously collected by the phone, that means the user was in proximity to someone who has tested positive.

The design choice meant that the infrastructure would not collect personal user information or track users—nor would the apps using the infrastructure be allowed to do so. Keeping proximity information on users' phones and letting the user decide whether to inform public health officials if they receive an exposure notification protect user privacy—but do so at a cost

of failing to provide public health officials with data regarding the rate and nature of exposure. Such data would have been particularly useful at the start of the pandemic, when little was known about how SARS-CoV-2 spread.

The apps do not report time or location of exposure; indeed, the apps are designed to prevent anyone, including the user, from finding out such information. Even so, public perception of the apps was often negative, undoubtedly in part because of distrust in how technology companies and the government have stretched uses of peoples' data beyond the original collection purpose. The GAEN protocol's complexity makes it not entirely easy to explain; and the large amounts of misinformation surrounding the pandemic likely played a role as well.

EFFICACY AND OBSTACLES

Exposure-notification apps can be exceedingly useful (*2*). Although the app's anonymized design prevents tracking who received notifications and acted on them, a study provided statistical estimates indicating that between 178,000 and 399,000 cases were averted through use of the UK National Health Service GAEN-based COVID-19 app in October through December 2020 (*2*). Exposure-notification apps speed up notification of exposure and pick up encounters that a user might miss—the people standing nearby during a conference break, the person alongside them on the subway.

But in this pandemic that has demonstrated a devastatingly disproportionate impact on certain communities, because the apps only run on the most recent iPhone and Android phones, many had anticipated that use of exposure-notification apps would prove problematic to low-income communities and the elderly for economic reasons. Early evidence shows, however, a somewhat more complex set of interactions. A study of the UK app showing decreased incidence of SARS-CoV-2 spread noted that regions of higher app use had “lower levels of poverty, are more rural, and have higher local GDP” (*2*). In those regions, the populations that use the apps are more likely to be white, but also more likely to be elderly.

The reasons behind low app use by marginalized populations involve more concerns than simply access to the right version of smartphone. A recommendation to isolate is markedly different for a low-income worker who has a role that requires physical presence and cannot afford to lose their job than for a middle-class person whose work can be done from home. Research has

¹The Fletcher School and School of Engineering, Department of Computer Science, Tufts University, Medford, MA 02155, USA. ²Department of Computer Science, University College London, London, UK. Email: susan.landau@tufts.edu

identified at least three reasons for failure to quarantine and isolate: need to maintain salary, need to buy essentials, and need for social services (3).

Reasons for failure to quarantine and isolate will also vary by demographic. For example, researchers found a high correlation between Massachusetts communities with high SARS-CoV-2 infection rates and those with three factors: high immigrant populations who are often reluctant to seek government aid, including health care, even when ill; a high percentage of people working in food services (exposing workers to high numbers of people); and individuals living in multigenerational households (4). People who fear involving

in eastern Arizona, home to about 12,000 members of the White Mountain Apache Tribe. Yet, despite struggles with poverty and chronic disease and many people on the reservation being infected by SARS-CoV-2, a tailored intervention by the medical team early in the pandemic at the Whiteriver Indian Hospital kept the death rate low (6).

Two responses were particularly valuable. First, families on the reservation often live in multigenerational settings, and this highly contagious disease could spread easily between members. So if one person was sick, contact tracers would immediately test oxygen saturation levels for everyone in the household, quickly picking up anyone else who might already be suffering serious

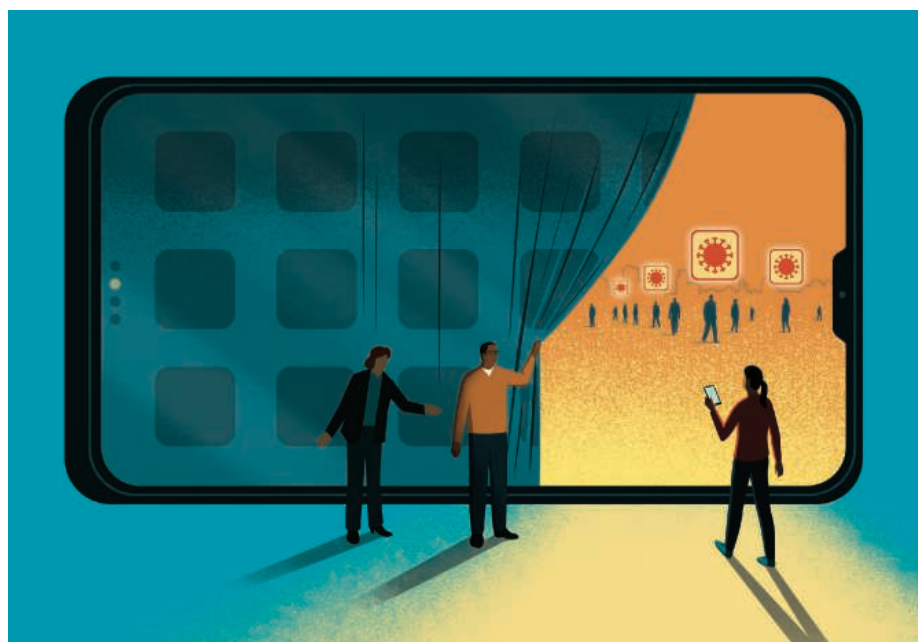
in marginalized communities where developing partnerships with churches, nonprofits, and community organizations—connecting with the connectors of the community—and being hands-on in providing care—access to testing, food, transportation, and treatment—were critical, whether in halting an eruption of syphilis cases in Baltimore in 2004 or responding to an Ebola cluster in Dallas in 2014 (7). Actions such as these create the trust that enables people to share crucial information on who might have been exposed to the disease and who might already be ill; it creates the willingness and capability to isolate despite the personal hardship.

Exposure-notification apps assume that users can manage the complexities of exposure and isolation. There are many for whom such an assumption just does not hold true (8). Thus, these apps provide neither the emotional support that human contact tracers do nor the encouragement and assistance that lead to patients' trust and willingness to list their contacts (9). In that sense, the exposure-notification apps are designed for a user who can handle the complexities that weeks of isolation may create—but not for someone for whom the logistical arrangements and economic consequences may cause household arrangements to capsize.

In light of this, economic support is crucial. The Swiss government financially supports those who receive a public health recommendation to isolate and who cannot work from home. Such aid is not only humane; it can be cost effective. One estimate from Massachusetts suggests that by decreasing the number of infections in the state, government support for quarantine and isolation would actually reduce government costs (3).

There is also the support that actually allows someone to isolate safely at home. Contact tracers ask: Are you safe isolating? What do you need? Do you need help with getting food or medication? Then the contact tracers go about ensuring that these needs are met.

The GAEN-based apps were intended to support contact tracing. Indeed, the Republic of Ireland's app, Covid Tracker, provides an option of registering with a phone number; in the case of an exposure, a contact tracer will call the exposed person, check how they are feeling, see if they need support when isolating and whether they are safe in doing so, and trace their contacts (10). In September 2020, Google and Apple introduced EN Express, which provides a menu of options enabling states to easily set up an app. But EN Express fails to include an option allowing the user to register



the government in their affairs and who are unlikely to be able to stay home from work because of a possible SARS-CoV-2 exposure are unlikely to benefit from an exposure-notification app.

Cultural history and socioeconomic challenges are different for distinct population groups. This then plays out in how likely contact-tracing apps are to be used. For example, a history of mistreatment has created great distrust of both the government and public health by many in the US Black community. That distrust is likely to undermine uptake of exposure-notification apps by many in this community. That said, exposure notification is more likely to be adopted by a middle-class person living in an integrated neighborhood than by a low-income individual living in a community with overpolicing (5).

The story about the coronavirus is different on the Fort Apache Indian Reservation

signs of the disease. Second, contact tracers, working in the knowledge that children in Apache families often have extended visits with nonresident grandparents, would ask, "Who are your grandparents?"—and then check on their health, even if they did not live in the same household (6).

ENABLING EQUITY WITH DIGITAL APPS

Exposure-notification apps provide benefits, but they can also exacerbate health care inequities. In a situation of scarcity—and for much of the pandemic, testing and medical attention have been scarce—testing driven by contact tracing in some communities can divert health care resources from people in other, marginalized communities.

The apps themselves are not contact tracers. Effective use of apps thus starts with contact tracers who are trained to be attuned to community needs. Contact tracers can point to success after success

their phone number—and that eliminates the possibility of automatically pulling in a contact tracer if a user has been exposed to SARS-CoV-2.

The current set of exposure-notification apps are designed so that an exposed person must reach out to public health officials rather than contact tracers reaching out to the exposed person. Populations with distrust of public health services and government are less likely to take that initial step. To provide people in such communities with the support that enables them to isolate and that creates the trust that allows tracing of their contacts, exposure-notification apps would be most effective if providing a contact phone number was the default.

That means an exposed person would become known to public health officials. The user, however, would have a choice whether to provide a number when downloading the app (and thus preserve their anonymity in the event of exposure). And even if a user does provide a phone number, the exposure-notification app would not be a centralized data collection service; it would provide public health officials with information that someone has been exposed—but not by whom. Information about which users were in someone's proximity would still remain on a user's phone. The only change that would occur by including a phone number would be automatic involvement of contact tracers in the case of exposure.

Providing a contact phone number should always be at the user's choice. An appropriate nudge during app signup indicating that providing a phone number would enable easier access to testing and social services could be used to encourage more users to do so. For privacy's sake, the system should be designed to ensure that opting out from providing a contact phone number is easy and explicit. If a user provides a number but later decides to opt out, doing so should similarly be simple. There should be no penalty for any user who fails to provide a contact phone number or later decides to remove it.

Providing a contact number removes the anonymity the user of an exposure-notification system would otherwise have, so other changes are needed to create trust in the system. Because false positives of exposure can have a disproportionate effect on those who can't easily isolate, app adoption should always be a user's choice (11–14). That right should also be legislatively guaranteed.

“Public health resources should be adjusted so that those demographics that are ‘underusing’ the apps do not lose needed resources.”

Though no one would learn the details of exposure—that is, the where, when, or by whom of exposure—exposures would no longer be anonymous for those who provide a phone number to the app. Thus, to ensure trust in the system—and adoption by people at risk—there would need to be strong policies protecting privacy of the data.

The apps don't distinguish between two people in close proximity in a small room—high risk of contagion—and being in close proximity outdoors, where risk drops substantially. Signal strength—and the corresponding measure of likelihood of exposure—varies depending on whether the phone is in a pocket or a handbag and could also vary by phone model and shape of a room (15). Bluetooth low-energy signals travel through building materials, which can lead to other false notifications of exposure, especially for those living in tightly packed housing.

Such false positives of exposure are problematic for everyone. But if false positives of exposure are having an inequitable effect on certain communities because of their inability to isolate and work from home, then there should be protections that ease the impact. These could include easier access to testing (and thus return to work), easier access to social services, and possibly even increased job protections for those who receive recommendations to isolate.

Information regarding exposure should only be used for contact-tracing purposes. Switzerland's Epidemic Act already does this, prohibiting disclosure of SwissCovid data for any other purpose; Australia does the same. Other countries should pass laws that information provided by contact-tracing and exposure-notification apps is to be used only for informing patients of exposure.

Use of the app should also be voluntary. Originally the use of Singapore's TraceTogether was purely at people's discretion. But in May 2021, the government effectively changed policy, requiring app use for entry in many Singaporean establishments, including shopping malls, restaurants, offices, and schools.

The GAEN-based approach is privacy protective, and early results demonstrate efficacy (2). The pandemic, however, exposed great health care inequities across different demographics. To understand how use of the app is affecting public health and what adjustments must

accordingly be made, apps must be tested before use. Communities experienced the pandemic in various waves; peoples' needs and behaviors have ebbed and flowed with the changes in risk. Thus, the apps must be tested repeatedly during public use, and this must be done across multiple demographic areas (11–14). Public health resources should be adjusted so that those demographics that are “underusing” the apps do not lose needed resources.

In every age, we expand our understanding of the causes of pandemics, their transmission mechanisms, and potential techniques for ending them. Exposure-notification apps provide a useful way to slow the spread of SARS-CoV-2. Like any technology, they change the dynamics of the disease's spread. This pandemic will not be the last that humans face. We must use and build tools and supporting health care policy so that the technologies are not only protective of people's rights, health, and safety, but also so that their use enables greater health care equity. Only then will the tools properly address both the medical and social occurrences of the pandemic. ■

REFERENCES AND NOTES

1. Government of Singapore, TraceTogether, Safer Together, www.tracetgether.gov.sg (accessed 15 April 2021).
2. C. Wymant et al., *Nature* **594**, 408 (2021).
3. M. Bourdeaux et al., “Estimating the costs and benefits of supported quarantine and isolation in Massachusetts: The missing link in Covid-19 response,” Faculty Research Working Paper Series RWP21-003, Harvard Kennedy School, February 2021.
4. J. F. Figueroa, R. K. Wadhwa, D. Lee, R. W. Yeh, B. D. Sommers, *Health Aff. (Millwood)* **39**, 1984 (2020).
5. S. Landau, *People Count: Contact-Tracing Apps and Public Health* (MIT Press, 2021).
6. R. M. Close, M. J. Stone, *N. Engl. J. Med.* **383**, e15 (2020).
7. C. P. Chaulk, J. Zenilman, R. Bialek, A. Rompalo, *J. Public Health Manag. Pract.* **27**, 322 (2021).
8. L. Smith et al., *BMJ* **372**, (2021).
9. S.-W. Jian, H.-Y. Cheng, X.-T. Huang, D.-P. Liu, *Int. J. Infect. Dis.* **101**, 348 (2020).
10. Government of the Republic of Ireland, HSE, “Privacy and How We Use Your Data,” <https://www2.hse.ie/services/covid-tracker-app/privacy-and-how-we-use-your-data.html> (accessed 20 August 2020).
11. S. Landau, C. Lopez, L. Moy, “The importance of equity in contact tracing,” *Lawfare*, 1 May 2020, www.lawfareblog.com/importance-equity-contact-tracing.
12. K. “K. J.” Bagchi et al., “Digital tools for COVID-19 contact tracing: Identifying and mitigating the equity, privacy, and civil liberties concerns,” Edmond J. Safra Center for Ethics, Open Technology Institute, and New America, 2 July 2020.
13. Ethics Advisory Board, NHSX, Letter to Secretary of State, 24 April 2020, <https://nhsbsa-socialtracking.powerappsportals.com/EAB%20Letter%20to%20NHSx.pdf> (accessed 18 October 2020).
14. N. S. Guiliani, ACLU, Government Safeguards for Tech-Assisted Contact Tracing, 18 May 2020.
15. D. J. Leith, S. Farrell, *ACM Comput. Commun. Rev.* **50**, 66 (2020).

ACKNOWLEDGMENTS

This work was partially supported by National Science Foundation grants CNS 1923528 and CNS 1955805.

10.1126/science.abi9852

Downloaded from <https://www.science.org> on July 26, 2022

Digital exposure tools: Design for privacy, efficacy, and equity

Susan Landau

Science, 373 (6560), • DOI: 10.1126/science.abi9852

View the article online

<https://www.science.org/doi/10.1126/science.abi9852>

Permissions

<https://www.science.org/help/reprints-and-permissions>