Government Safeguards for Tech-Assisted Contact Tracing

By Neema Singh Guliani
May 18, 2020

As we continue to grapple with the COVID-19 pandemic, many governments are turning to technology in the hopes that it will help fill the gaps in public health resources. In particular, governments around the world are exploring whether technology can be used to assist with contact tracing. This would involve the use of technology to identify who may have come in proximity with an infected person and to notify them. These tools are different from traditional contact tracing, long used by health professionals, which typically relies on information from individuals to manually contact people who might have been affected.

As we have noted previously, some contact tracing technology proposals should be dismissed outright: They won't work and are inconsistent with democratic principles. For others, like the Google-Apple proposal, further exploration is needed to determine if the tools are effective, practical, and worth the many tradeoffs. Regardless of where we land on these questions, it is clear that the deployment of any of these tools in the U.S. will require additional legal protections and governance structures to ensure that they are used effectively, as intended, and consistent with existing law.

In previous papers, we discussed the limits of various technology-assisted contact tracing proposals and the general technology principles that should guide the consideration of any proposal. But while efficacy and technology principles that embed privacy by design are necessary, they are not sufficient to ensure properly limited use of technology to assist COVID-19 contact tracing efforts. In this paper, we outline some of the safeguards governments should adopt to guard against overreach and abuse, and build user trust.

Many of these additional safeguards are also applicable to other efforts to deploy technology to combat the pandemic. At a minimum, if a contact tracing app or technology is used, state and local governments and companies should adopt strict policies and procedures that ensure:

- **Effectiveness:** Governments should evaluate and set benchmarks for efficacy of the technology, factoring in accuracy, risk of false positives/negatives, and known limitations.
- **Voluntary Use**: Governments should ensure that any use of a contact tracing app or technology is voluntary. Important public benefits, such as immigration, food stamps, housing assistance, and the like, should not be conditioned on use of a contract tracing app. And governments should prohibit private and public entities from making the use of a contact tracing app or technology a condition of access to employment, public transportation, housing, and other necessities and critical services, such as grocery stores and pharmacies.
- **Equity:** Governments should proactively develop projections and plans to target deployment of additional health resources to communities that lack the tech and other support needed to use a contact tracing app. Use of aggregate data, with appropriate privacy protections, can help governments identify such communities.
- **Use Restrictions:** Governments should require that any data obtained from these tools may be used only by public health agencies and for public health purposes related to the pandemic, and should be destroyed after its use expires.
- **Enforceable Rights:** Governments should commit to using only apps with terms of service that provide strong enforceable privacy protections. Technology developers should also commit to providing such protections, and distributors of technology (like Apple and Google) should limit their distribution to technology that is accompanied by these protections.
- **Transparency, Oversight, and Accountability:** Governments should adopt independent auditing and oversight measures to ensure that any contact tracing app is used solely for public health, operates as intended, and is limited to the duration of the pandemic.

Even if these tools are adopted with appropriate safeguards, it is important to recognize that they are far from a silver bullet. They will not resolve testing shortages, which are essential for notified individuals to determine if they have in fact been infected. They will not ensure individuals who are infected get adequate and equitable treatment. And they are not a substitute for clear guidelines for the public to determine what they can do to better protect themselves, their families, and their communities. Thus, these tools can only be part of a broader health strategy that resolves these and other significant issues.

Effectiveness

Contact tracing or related technology should be deployed only if it promises to be effective, and should continue to be used only if it is shown to work. At this time, there is not sufficient information to conclude that the proposed tools will be effective, a good use of resources, or practical. It is also unclear what benchmarks public health agencies will use to measure effectiveness and thus whether it is appropriate for a contact tracing tool to be part of a

broader COVID-19 public health strategy. The last thing we need is technology being improperly relied on, wasting health resources, or creating more confusion. In other contexts, we have already seen how failure to apply accuracy and effectiveness benchmarks may be adversely affecting public health outcomes. For example, many have expressed concerns that inaccuracies in antibody testing could give individuals a false sense of security or be improperly relied on to make public health decisions. This problem is further exacerbated by the lack of certainty over what, if any, immunity may be conferred to individuals who test positive for antibodies.

To prevent improper reliance on contact tracing or related technologies, health agencies should set clear public benchmarks for what standards a tool must meet to be considered effective. These benchmarks should consider factors that impact effectiveness, overall rates of accuracy for notifying individuals of potential exposure, and any limitations of the technology. Information should be made public about how these tools measure against these benchmarks so that the public has a clear understanding of how and whether they are reliable. To the extent public health agencies contract with developers to create these tools, the developers should be required to provide the necessary information to conduct this analysis.

Voluntary Use

In order to be effective and maintain trust, it is crucial that any contact tracing tool used to fight the pandemic be voluntary. Public health experts have found that coercive health tactics frequently backfire, sparking counterproductive efforts by people to resist and undermine health measures. For the app to work effectively, people must be able to trust that any digital contact tracing tool will not be used to harm them. Ensuring that use is voluntary is essential to building the trust necessary to make contact tracing work.

Trust through voluntariness is particularly important because contact tracing apps won't be effective if infected individuals resist supplementing the data collected with their personal knowledge. Even if widely used, contact tracing apps will have to be supplemented by more traditional contact tracing, conducted through interviews. For example, the Apple-Google proposal — which would use Bluetooth proximity to alert individuals that they may have been near someone infected with COVID-19 — has several blind spots. It might not detect when an individual is in a car — and thus unlikely to have infected others outside the car. It does not factor in other features of an individual's behavior — such as interactions without protective gear or intimate encounters — that *increase* the likelihood of transmission. And it is unable to identify any behavior that occurred when a phone was left at home or turned off. Additional personal knowledge will thus be critical in making sure that tools genuinely assist contact tracing efforts. And again, voluntary use is critical to obtaining cooperation in this effort.

Recognizing these realities, to their credit, some of the proposals to create contact tracing or related technologies have emphasized that use of such a tool must be completely voluntary.

For example, the Apple-Google draft proposal emphasizes the central role that consent must play in the successful deployment of any contact tracing tool. However, more needs to be done.

There are a variety of actors who can coerce individuals into using a contact tracing app. Employers, landlords, or even private business owners may require use of the tool as a condition of employment, tenancy, or even access to basic necessities, such as grocery stores, pharmacies, and other critical services. Government officials might also condition access to important public benefits, including immigration benefits, food stamps, housing support, and the like, on use of a contact tracing app. But these would be coercive, not truly voluntary.

Surveillance often hits vulnerable communities the hardest. For example, many public benefits are conditioned on the disclosure of sensitive personal information — sparking fear in many immigrants who worry this information might be funneled to immigration enforcement agencies. Face recognition technology has already been deployed in some public housing, absent tenant consent, public use policies, or even basic privacy protections.

Efforts to coerce individuals to use contact tracing or related technologies are also particularly concerning because they may run awry of existing civil rights obligations. Millions of individuals will lack the technology and ability to use the tool. In such cases, conditioning access on use of a contact tracing app may deny equal access to employment opportunities, housing, or other basic necessities or critical services. In addition, depending on what data is collected and generated by such technologies, compulsory efforts could violate existing laws that prohibit employers from asking about health conditions as part of the hiring process or in cases where such conditions are unrelated to an individual's ability to perform a specific job function.

To safeguard our civil rights and prevent the public risks posed by coercive contact tracing or related technologies, it is essential that we take additional steps to ensure that any use of such tools is voluntary. Governments should make clear that government benefits or services, including immigration benefits, are not conditioned on use of contact tracing technologies. Governments should pass legislation or issue guidance that similarly instructs private employers, landlords, business owners, and others to not condition access to basic necessities and critical services on the use of a contact tracing technologies. Developers of contact tracing technology should also exercise their discretion and only contract to create products on behalf of public health agencies that have adopted these policies. Finally, governments should create accessible mechanisms through which individuals can submit complaints related to violations of such guidance, so that they can be appropriately investigated and enforced.

Equity

It is not clear yet whether any contact tracing tool will be effective. However, it is clear that if governments rely on these technologies as the sole means of contact tracing, they will exacerbate existing health inequities and undermine our overall ability to prevent community transmission. Data on the COVID-19 outbreak in the United States shows that Black

communities have been disproportionately afflicted, as have other communities of color. Any solution that does not specifically ensure that those communities will be helped will thus exacerbate existing racial disparities in the effects of COVID-19.

Many of our most vulnerable community members may be unable or unwilling to use a contact tracing app, which requires a smartphone. Studies have found that over 40 percent of individuals over age 65 do not have a smartphone — a population that accounts for over three-quarters of COVID-related deaths. Similarly, nearly 30 percent of individuals earning less than $30,000 annually do not own a smartphone, individuals with disabilities are 20 percent less likely to own such devices than the general population, and additional subgroups, including people who are homeless or incarcerated, may also lack access. Affordable internet connectivity may also pose a challenge to using a contact tracing app, given the need to transmit data, with Pew estimating that 24 million Americans and 30 percent of rural Americans lack access to broadband service. Even for those who have access to a smartphone and affordable broadband, technical capability and lack of support may pose a challenge.

Indeed, the case of Singapore offers a cautionary tale regarding ignoring the health needs of particularly vulnerable populations. The country's resurgence of COVID following a downturn has been driven in part by rising cases in Singapore's vulnerable migrant communities, where people are forced to live in poor conditions that prevent them from being able to take necessary safety precautions. Early numbers estimated that these areas accounted for 70 percent of the country's new infections. In studying the resurgence, many have noted that Singapore failed to address cramped migrant living conditions or to put in place large-scale testing in migrant communities. As a result, the country underwent a lockdown in an effort to slow the spread of the disease. Similarly, within the United States, public health officials have warned about the community impact of failing to address disease spread in vulnerable areas. For example, experts project that failing to take steps to prevent the spread of disease in prisons could result in 100,000 more deaths than some models projected. Similarly, modeling has shown that surges in infections in immigration detention facilities would quickly overwhelm ICUs in neighboring communities.

Given this reality, use of a contact tracing or related technologies should be coupled with a broader plan designed to ensure robust traditional contact tracing methods, testing, and treatment for our most vulnerable communities. At a minimum, this should involve publicly available pre-deployment assessments about which populations are likely not to use a tool. Using these projections, governments must invest in alternative contact tracing efforts targeted specifically at communities that may not reap the potential benefit of a contact tracing technology.

Additionally, health agencies, in partnership with the private sector where appropriate, should ensure that any rollout of new technology is coupled with efforts to provide technical assistance to those who may need it. In particular, communications about the tools, including information about privacy, should be in plain language and written at a fourth-grade reading

level (or less) to reach the widest audience. Materials on websites should be accessible to screen readers and other assistive technologies, and consistent with WCAG 2.0 AA standards, and televised announcements should include closed captioning and a qualified American Sign Language (ASL) interpreter. Moreover, appropriate guidance and information should be provided to health professionals so that they best advise patients on use.

While governments bear the ultimate responsibility for providing equitable health access, the private sector can assist with these efforts by providing information on how localities can use data, surveys, and other tools to project app adoption rates by community. With appropriate privacy protections, ongoing aggregate information could also assist in identifying where to target additional health resources.

Restrictions on Use

For people to feel safe and secure using contact tracing apps and technology, it is essential that any information gleaned from these tools be used solely by public health agencies and solely for public health purposes during the pandemic. It should not be used by private companies for commercial purposes, or for criminal or immigration enforcement purposes. And it should be destroyed once its use has expired. Just as with mental health and substance abuse treatment, failure to keep information confidential could dissuade individuals from seeking essential health treatment.

As we have emphasized before, the best way to ensure these limits are in place is to adopt design features that put users in full control and limit the transmission of data to a central repository. Recognizing the importance of limiting the use of information, many proposals related to contact tracing apps or technology also limit use of the technology to public health agencies. However, to provide full protections, governments should adopt regulations or laws that strictly limit use of information gained from these tools for public health purposes, prohibit disclosure of personal information to non-public health agencies, and require destruction of the data once its utility has expired.

Enforceable Rights

Many of the proposals surrounding contact tracing technologies have emphasized the importance of strong privacy protections — including limited data collection, requiring user consent, and cessation of all technology-assisted contact tracing efforts when the pandemic ends. Again, good design features that limit data collection and put users in control of their data is the best way to ensure limits are in place. However, even with good design features, some information will likely still be collected, and individuals will need a way to enforce their rights in cases of abuse or inadvertent error.

Unfortunately, our existing laws are insufficient to protect rights in all contexts where these tools may be used. Health privacy laws, like the Health Insurance Portability and Accountability Act (HIPAA), generally do not apply to health data generated by private consumer apps and devices, and the federal government has waived the law in certain COVID-19 contexts. At the same time, the United States lacks a strong, comprehensive federal data privacy law that would protect consumers' rights. At the state level, there are a patchwork of privacy protections that largely fall short.

Thus, to ensure that individuals who use contact tracing technologies have enforceable privacy rights, public health agencies should only use or contract with companies that have strong privacy protections built into their terms of service. Those terms should:

- Notify users in plain language of what information is being collected and how it is being used;
- Limit data collection, use, and retention to what is necessary to provide the contact tracing service being provided;
- Permit use and transfer of information only to public health agencies and only for public health purposes, safeguarding information from law or immigration enforcement officials;
- Require specific opt-in consent to transfer any data from the user's device;
- Prohibit surreptitious collection of location and other information without the user's specific opt-in consent;
- Require any health agency that receives data to limit subsequent transfers without the user's specific opt-in consent;
- Exclude provisions, like mandatory arbitration, that make it difficult for individuals to seek redress in cases where terms of service are violated;
- Permit a consumer to request information about personal information that has been collected, used, or retained about them, and to delete it; and
- Cease functioning and delete personal data based on specific criteria that indicate the pandemic has ended.

As we move forward, public health officials may also identify additional protections that are needed to address the inherent privacy concerns with any type of contact tracing, given the risks that individuals contacted may be able to infer others' health status.

Distributors of apps, like Google and Apple, can also take important steps to ensure that appropriate privacy protections are built into tools available in their store. For example, both Google and Apple have developer policies that provide guidelines for technical and privacy standards that must be met for apps available in the Apple App Store and Google Play. These developer policies should be augmented to require that contact tracing apps meet the privacy standards articulated above.

Transparency, Oversight, and Accountability

Governments will need structures in place to ensure that any contact tracing or related technology is used as promised, is a wise use of government resources, and complies with existing policies. While many public health agencies may rely on private companies to develop these tools, they must not completely outsource these important responsibilities.

We have already seen examples of technology that was purportedly designed to help the COVID-19 public health efforts backfire. For example, in early April, Utah deployed a system that was supposed to alert people entering the state that they should complete a survey with their name, address, phone number, email, and any potential symptoms or exposure to COVID-19. Three days later, the Utah Department of Emergency Management suspended the system after it became clear that it did not work; numerous individuals mistakenly received the alert though they were nowhere near one of the nine virtual checkpoints or were in fact leaving the state. To prevent similar waste of resources, state and local governments will need to take additional steps.

First, they should designate an independent entity to conduct regular audits during the use of an app. This should involve assessments about whether the privacy practices line up with policies, including restrictions on transfers and collection of information. In addition, the audits should assess whether use of the technology fully ceases when the pandemic ends and whether data is appropriately purged.

Second, government agencies should provide opportunities for community input, including by those hardest hit by the pandemic, on any technology prior to and after deployment. In 13 jurisdictions, including San Francisco, California and Seattle, Washington, existing law already requires that new surveillance technologies be subject to public debate and approved by legislatures. These laws should be strictly followed. In other places, government agencies should ensure similar protocols are in place that provide the opportunity for public input and legislative approval where appropriate.

Finally, the government should adopt a policy of proactive transparency. This should include full public release of contracts related to development of the technology, audits, and agency guidelines governing the treatment of any information related to the tool. This transparency is essential to maintain public trust and ensure that individuals can feel confident that their rights are being fully protected.

Conclusion

Given the seriousness of the pandemic, we should fully debate and consider technological tools that may have efficacy. And, as has already been demonstrated, the private sector can play an important role in developing novel approaches to combating the disease. However, we must recognize that new technological tools will also require additional actions by governments to

maintain public trust, ensure new technology is used as intended, avoid exacerbating existing racial disparities, and to protect our fundamental rights. Thus, governments considering the use of contact tracing or related technologies must take steps to ensure voluntary use of any tool, ensure equitable health resources, limit use of any data obtained to public health purposes, provide individuals with enforceable rights, and maintain appropriate oversight, accountability, and transparency.

###