Accepted Commentary – In Press

Contact Tracing: Can 'Big Tech' Come to the Rescue, and if so, at What Cost?

Pratik Sinha MD PhD[1,2], Alastair E Paterson[3] M.Eng

1. Pulmonary and Critical Care Medicine, University of California, San Francisco, CA, USA
2. Department of Anesthesia, University of California, San Francisco, CA, USA
3. Chief Executive Officer, Digital Shadows Inc, San Francisco, CA, USA

Corresponding Author:

Pratik Sinha

505 Parnassus Avenue, M1088

San Francisco, California, USA

pratik.sinha@ucsf.edu

Word count: 1096

COVID-19 has resulted in a unique amalgamative failure of economics, healthcare, and society. Without an effective vaccine, the precise mechanism to resuming "normal" activity remains unknown. Public health consensus seems to align on the need to test, trace and isolate infected individuals with a stepwise repeal of lock-down measures. The infrastructure for contact-tracing, however, are woefully underdeveloped worldwide. In the US, it is estimated that 180,000 contact-tracers would be required and only 0.5% of that number currently exist.[1] Moreover, incumbent programs are built to trace slow moving infections and are not fit-for-purpose for this pandemic. Theoretically, Big Tech (large technology companies) can provide innovative solutions to address some of the unmet challenges of contact-tracing. These solutions may seem intuitive; however, they pose a significant risk to digital security and patient privacy. Outlined below are some of proposed methods for digital contact-tracing and the threats they pose.

Broadly speaking, four categories of applications (apps) are being proposed for digital contact-tracing (**Figure)**. Technical specifications aside, they vary from one another by the degree of invasiveness in terms of privacy. The more likely contenders are based on using smartphones' location data and Bluetooth interactions to enable contact-tracing. A critical decision for developers of contact-tracing apps is whether to publish the source code ('open-source') or keep it private ('closed-source'). Closed-source software are considered a higher risk as they cannot be scrutinized for security flaws by third-parties. They have unknown privacy implications since the inner-workings of the apps will only be known to developers. Algorithms may run in the background collecting unconsented data. Open-source apps have the theoretical disadvantage of delayed deployment as the codes undergo external scrutiny.

A critical decision for healthcare systems using such apps is whether to store the collected data in centralized repositories or locally at the device level. Centralized data collection in 'trusted' platforms comes with associated privacy concerns since governments would potentially have access to citizen's

location data, the 'social graph' of all physical contacts, and any other data the app is able to access from the phone. The track record of data loss from centralized government agencies is also a significant concern. Worryingly, many countries including China, Russia, U.K., Norway and Vietnam are taking a closed-source approach to developing their apps and using centralized frameworks. The Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) is another closed-source initiative backed by at least seven European countries including France and Italy.

The trade-off between surveillance and intrusion has always been a balancing act, especially in the post-911 era as governments desire broader access to prevent terrorism, while civil liberties groups protest overreach into private lives. Maslow's Hierarchy dictates that health comes first. Nevertheless, privacy advocates are understandably concerned about how data are tracked and stored, who has access, and what happens to it when the pandemic is over. South Korean contact-tracing laws, for example, permit the government to ascertain immigration status of infected individuals. If such laws exist in the U.S., its implications may be two-fold. First, undocumented communities may not seek healthcare. Second, it is not inconceivable, that over time the same technologies and laws could be used to track undocumented migrants. Once a precedent is set, governments seldom trackback on powers granted to them in times of crisis. Highlighting these concerns, 200 UK scientists who wrote an open letter to the UK Government on April 29th stating "it is vital that, when we come out of the current crisis, we have not created a tool that enables data collection on the population, or on targeted sections of society, for surveillance".[2]

The lack of trust in apps has significant implications in their efficacy. First, it may diminish public enthusiasm for using them. It makes intuitive sense that app usage needs to exceed the prevalence of SARS-CoV-2 infection. It is estimated that approximately 80% of smartphone users will need to use an app for it to be efficacious.[3] Second, the lack of unanimous consensus of its utility may lead to unfounded

propagation of conspiracy theories and uncertainty. Governments, therefore, need to have greater transparency and provide clear assurances before individuals voluntarily use such apps. To that end, citing privacy and uptake concerns, Germany was originally part of the PEPP-PT but has recently switched to an open-source approach called DP-3T (Decentralized Privacy-Preserving Proximity Tracing), based on Apple-Google's decentralized application programming interface (API).

Apple-Google are proposing a decentralized model where data will be stored at the device level rather than centralized platforms.[4] Given Google Android and Apple iOS jointly possess almost 99% of the global smartphone operating systems, it seems likely that their approach will be critical in how the majority of contact-tracing apps operate. Given that this API is the leading global standard, it is worth studying it in greater granularity. Each phone will broadcast an identifier over Bluetooth at regular intervals and all nearby phones will record which other identifiers they can pick. Individual phones will regularly change their identifier, making it hard to track. Most data are stored on individual phones. Once infected, however, all the individual's generated identifiers in the preceding two weeks are released to an app running on this platform. Currently Apple-Google have no intentions of building the app themselves. Since no data is stored centrally until an individual is infected, API offers greater privacy than centralized platforms. In a departure from their usual indolence to data privacy, Big Tech companies are in this case advocating a more privacy-preserving model. Paradoxically, the government of France is currently in dispute with Apple and Google urging them to weaken incumbent privacy protections to help PEPP-PT. The resolution of this dispute will have widespread implications as it is likely to set the precedence for other countries. A limitation of the Apple-Google API is the concerns that these, already ubiquitous, tech giants would further consolidate their monopoly of humanity's digital footprints.

The implementation of these invasive healthcare digital technologies will likely lead to meaningful changes in laws that govern civil rights. The time-honored tenets of justice and autonomy in patient-care, however, should not be forsaken even in this pandemic. To that end, we advocate that at the very least, apps proposed by authorities should be transparent using open-source code with de-centralized platforms, as this offers a more acceptable balance between access and privacy. Further, like all healthcare interventions, contact-tracing apps need testing for efficacy and safety before widespread dissemination. The roadmap to scaling and implementation (**Figure**) of digital contact-tracing is complex and will requiring comprehensive socio-political buy-in. Technology is only part of this complex puzzle, however, when applied thoughtfully, it may be critical in restoring livelihoods in this pandemic.

Conflict of Interest: Dr. Sinha has nothing to disclose. Mr. Paterson is the Chief Executive Officer and co-founder of Digital Shadows Inc, a company specialising in digital risk protection.

References

1. Simmons-Duffin S. We Asked All 50 States About Their Contact Tracing Capacity. Here's What We Learned. NPR Apr 28, 2020. https://www.npr.org/sections/health-shots/2020/04/28/846736937/we-asked-all-50-states-about-their-contact-tracing-capacity-heres-what-we-learne
2. Albrecht M, Aparicio-Navarro F, Arief B, et al. Joint statement of U.K. scientist working in the field of privacy and security. 29 April 2020. (https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view)
3. Hinch R, Probert W, Nurtay A, et al. Effective configuration of Digital Contact Tracing App: A report to NHSX. 16 April 2020 https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf.
4. Privacy-preserving contact tracing. April 2020. (https://www.apple.com/covid19/contacttracing)

Figure. A framework for the ethical and transparent development and implementation of contact-tracing apps in the COVID-19 pandemic. The table is a summary of proposed contact-tracing app development approaches and data platforms currently being widely used in COVID-19.

Contact Tracing and COVID-19

Development

Source Code

Open Source:
- Enable third-party scrutiny
- Identify security issues
- Transparency builds trust

Data Handling

Collection:
- Informed consent
- Required data only

Storage:
- Decentralized at device level

Scaling

Collaborative:
- Shared learnings & pooled resources
- ↑ Scalability & security
- Cost efficient
- Increase power for testing efficacy

Implementation

Legal Issues

- Time bound law
- Data protected for intended purpose only
- Regulatory compliance
- Diagnosis by healthcare only

Efficacy

Prospective studies:
- Test technology effectiveness
- Determine accuracy of tracing contacts (sensitivity and specificity)

Uptake

- Transparency
- Public information
- Health campaigns

Type	Example	Auto-location detection	Based on Apple/Google API	Centralized Database	Notes
Self Reporting Apps	Kings College-backed 'C-19 COVID Symptom Tracker', Healthcast, ZeroBase	No	No	Yes	While they may provide useful research data and indicators if adopted widely, they are unlikely to be useful for contact tracing since they cannot automatically identify who the reporters have been in contact with or the veracity of their claims.
Custom-Built Closed-Source Location Tracking Apps and Frameworks	Norway, Russia, Vietnam, China, UK PEPP-PT (7 EU countries including France, Italy)	Yes	No	Yes	Lack of published, scrutinized source code increases risk of security flaws or hidden surveillance. Centralized database is at risk ofattack and data breaches. Not using Apple/Google API may cause battery life and other efficacy issues.
Open-Source Apps & Frameworks (not using Google/Apple API)	BlueTrace/OpenTrace (Singapore TraceTogether, Australia COVID-19 Safe). TCN Protocol, Israel	Yes	No	Yes	Published source code enhances security and trust, but centralized database may be open to attack and data breaches. Not using Apple/Google API may cause battery life and other efficacy issues.
Apps Using Google/Apple API	DP-3T (Germany, Austria, Estonia, Netherlands), California	Yes	Yes	No	Using Google/Apple API is the only way to use native operating system functionality which is lighter on battery use and better for location tracking. Lack of centralized database is good for privacy, but limits data deemed necessary by France and other countries' Governments.