Tech is not the Limit — Trust is: Why apps could not solve this crisis and will not solve the next

Earlier this year, many have debated how contact tracing apps should be designed. Yet, questions of data storage and system architecture have never been the primary problem: citizen and consumer trust is. Fewer than 50% of the smartphone-owning public reported that they would use tracing apps with 18% being non-users,[1], while more than 60% of the total population would be needed to contain outbreaks.[2] Under these circumstances, contact tracing apps are unlikely to ever work, and thus they failed as expected. People simply – and rationally – do not feel like they can trust Big Tech or government with their data, particularly not during a raging pandemic – and in these times of political uncertainty and unrest.

Architecturally, there are two categories of contact tracing apps: centralized apps where the data are stored by a central authority and decentralized apps that send and store data in a distributed manner. If implemented as promised, a decentralized app (most use the Google/Apple-supported privacy-respecting approach and API[3]) can prevent, or at least limit, the abuse of data. But this approach comes at the considerable cost of data accuracy and tracing effectiveness.

From a purely statistical and architectural perspective, a more centralized approach, (e.g., an app that uses proximity data and GPS or cell tower data), is more powerful at tracking the spread of disease; as a general rule, data analysis and tracing improve with more and better data (with diminishing returns). Central data analysis and storage would have given researchers more data to analyze, better estimates to prepare hospital resources, and more information to identify potential infection chains[4]. The more data we store centrally, however, the more valuable that data becomes, not just in context of tracing infection chains but for all kinds of uses.[5] A valuable data-set or system will lead to increased likelihood of external attacks but might also be used by its controllers

[1] https://seclab.cs.washington.edu/wp-content/uploads/2020/05/contact-tracing-user-privacy.pdf

[2] https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Centralised%20and%20decentralised%20systems%20for%20contact%20tracing.pdf

[3] https://covid19.apple.com/contacttracing

[4] https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app

[5] https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view

beyond the advertised mission statement. People will not trust centralized apps where data flows to an untrustworthy company or government; nor should they.

Clearly, the issue at the heart of this debate is not technology or system architecture. Whether we use (contact tracing) apps comes down to whether the American and international public believes that it can trust in the developers and controllers of these applications. We do not, and apparently cannot, discuss what would be the “best system” that provides the best balance of privacy and effectiveness. Instead, we face a lack of trustworthy institutions (public or private); and thus, our only realistic options appeared to be decentralized, low-data applications that are inherently less effective. Yet, even those technically privacy-respecting applications see close to no usage.

We got to this point because tech companies and governments have continuously eroded and dismissed privacy as well as civil liberties. Today, consumers appear to increasingly perceive Big Tech and government data processing as invasive and inappropriate. Thus, the question is: How can companies and governments reestablish that trust we need to actually make such applications work? For Corona tracing apps, it is already too late.

To get consumers to trust them again, companies and governments will have to demonstrate over time that they are trustworthy. A strategy to get people back on board will have to include transparency, opening up source code and demonstrating what goes into an application, clear privacy policies and controls (unlike current privacy policies), repercussions for anyone who fails to follow the rules, organizational barriers or data silos, and finally, actual consumer choice. Accountability and transparency measures can also help demonstrate to the public that an organization takes their concerns seriously, has clear and understandable rules, and most of all, sticks to their own rules and punishes those who misbehave.

Unfortunately, while all these things are useful, they are only stepping stones toward the greater goal of regaining public trust, after a change of heart has already occurred. Organizations and employees, including executives and policymakers, have to take responsibility for public interest and well-being. Tech companies and governments must accept that Silicon Valley’s culture, and the nation’s culture more generally, need significant and real change, not only due to recent events but also due to years of public interest concerns being ignored by both government and technology firms.

Without doubt, re-building trust will be difficult, as years of “more of the same” have eroded the relationships between citizens, government, and large private companies. (Privacy) rules must be clear, obvious, applicable, and followed in letter *and* in spirit, not just by consumers or citizens but also by powerful actors like law enforcement and well-resourced Silicon Valley giants. If citizens are not able to believe the promises of powerful institutions, there can be no trusted and therefore effective solutions for whatever digital tools we need to weather the next crisis.