Apps Gone Rogue:
Maintaining Personal Privacy in an Epidemic

Containment, the key strategy in quickly halting an epidemic, requires rapid identification and quarantine of the infected individuals, determination of whom they have had close contact within the previous days and weeks, and decontamination of locations the infected individual has visited. With almost half of the world’s population carrying a device capable of GPS tracking, location trails - timestamped logs of an individual’s location - can be created. By comparing a user’s location trails with those from diagnosed carriers of infectious disease, one can identify users who have been in close proximity to the diagnosed carrier and, if the exposed users take appropriate action, reduce the spread of the infectious disease. However, first-generation contact-tracing tools, deployed against the current 2019 novel Coronavirus (COVID-19) crisis, can also be - and have been - used to expand mass surveillance, limit individual freedoms and expose the most private details about individuals. Citizen-centric, privacy-first solutions that are open-source, secure, and decentralized (such as MIT Private Kit: Safe Paths) represent the next generation of tools for disease containment in an epidemic or pandemic.

Private Kit: Safe Paths is an MIT-led, free, open-source and privacy-first contact-tracing technology that provides individual users with information on their interaction with diagnosed COVID-19 carriers, while also empowering governments’ efforts to contain an epidemic outbreak. The Private Kit: Safe Paths solution, in its first iteration, enables individuals to log their own location on their own phones. With consent, diagnosed carriers can share an accurate location trail with health officials once they are diagnosed positive, replacing a process that has historically been conducted only through memory. In its second iteration, Private Kit: Safe Paths provides users with information on whether they have crossed paths with a diagnosed carrier. Governments are equipped to redact location trails and thus broadcast location information with privacy protection for diagnosed carriers and local businesses. In its third iteration, Private Kit: Safe Paths enables privacy-protected participatory sharing of location trails of diagnosed carriers and direct notification to users who have been in close proximity to a diagnosed carrier, without allowing a third party, particularly a government, to access individual location trails. Private Kit: Safe Paths' ability to provide contact-tracing without collecting information on the user in an external cloud prevents government surveillance, and, as an open-source tool Private Kit: Safe Paths fosters public trust.

Securing the privacy of individuals, diagnosed carriers, and local businesses visited by diagnosed carriers, while still informing users of potential interactions with carriers remains the primary challenge for contact-tracing technologies. Several steps may be taken to mitigate these risks. Private Kit: Safe Paths reduces the risk of privacy violations by replacing centralized storage of sensitive data with time-limited storage of data on the user’s own device and requiring user consent for data sharing. Other issues, such as access and inclusion for non-smartphone owners and marginalized populations, are not easily resolved. However, implementation of contact-tracing technology within a community, even with these limitations, may increase the safety of all as containing an epidemic outbreak quickly benefits everyone within a community through the epidemic’s peak and decline.

Traditionally, an inverse relationship existed between the quality of the data analytics and privacy for contact-tracing, however Private Kit: Safe Paths is both high privacy and high accuracy. Whereas containing an epidemic formally necessitated compromises by the user community, Private Kit: Safe Paths offers an opportunity to fundamentally alter this relationship. Private Kit: Safe Paths draws on the advantages from several models of contact-tracing technology while better mitigating the challenges posed by the use of such technology. Most importantly, it eliminates the risk of government surveillance.