TRANSPARENCY AND CONSENT - BY DEFAULT

Authors: *Ramesh Raskar, Deepti Pahwa*

Surveillance State, or a Better Option?

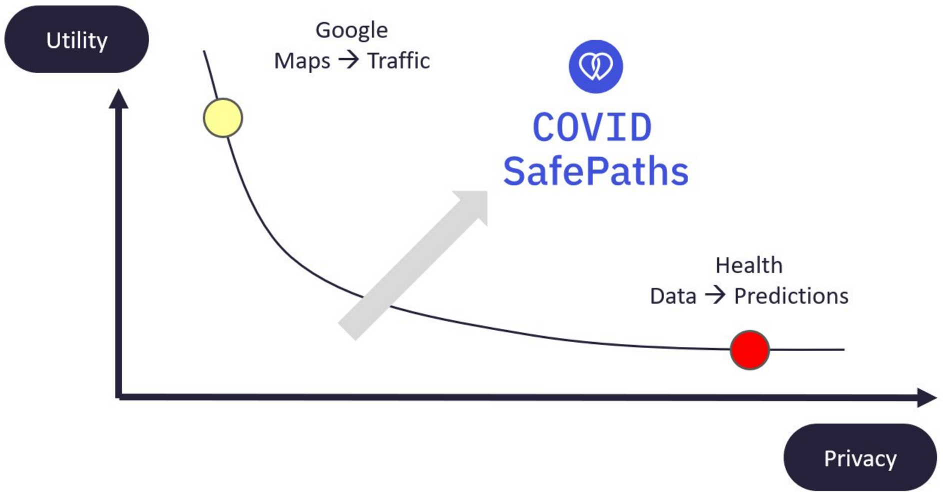
Difficult times lead to clear perspectives. The coronavirus (COVID-19) pandemic has stopped “life as normal” across much of the world. As governments and healthcare systems put into place strict measures around movement to slow the rate of infection and minimise the death toll, we are coming into a period of significant citizen uncertainty. Managing the outbreak of COVID-19 and flattening the curve is now a global challenge. WHO recommends tracing potential contacts of diagnosed COVID-19-infected patients as a base for targeted interventions such as “quarantine” or “testing” to contain the virus.

We read about contact tracing a patient in Korea, Patient 31, a woman who went to the hospital after a car accident, went to a hotel buffet, attended a church, came back to the hospital, and in turn ended up impacting more than a thousand people. The health authorities and contact tracers had to painstakingly interview more than a thousand people to back-trace and see who could be at risk to avoid further spread. Now, this type of social network analysis done manually is nearly impossible and prone to human memory errors. Digital interventions in such a case can lead to a surveillance state. Have we formed our perspectives on what is the best way forward?

Digital Dilemma: Utility, Safety, or Privacy?

Through digital contact tracing, we can warn individuals if they crossed paths with a person who has COVID-19 and make the process efficient by reducing the time it takes to inform them. We can help them isolate or take care of themselves if they're part of the at-risk population. This can be very easily done by using phones, with the help of GPS and Bluetooth, to compute the proximity of a healthy person who might have come in contact with a person who has COVID-19. This concept is already prevalent. If you use tools like Google maps, you know it allows you to see who else is around you and where there is traffic. The reds and the greens give you a safe path. And the reason this is possible is because we have very few privacy frameworks built-in. We willingly give away our location to Google and we get great utility out of it. We make this privacy trade-off to understand the traffic around us and the convenience it provides to us.

But when using a similar system for contact tracing, do we need to know “who” is the person who has COVID-19 around us, or simply that “someone” is infected? Do we need to know “where” that infected person lives, or just our own “safe path” that avoids our risk of getting infected? Is there a way to intentionally design an intelligent system of contact tracing with human-centricity and privacy at its heart?



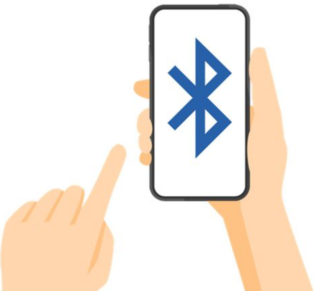
When it comes to health data, as in this case about infections and public health, we are very careful. We know that all the data is siloed and we have to be concerned about privacy. The ambition, at the same time, is also to utilize the data. In some Asian countries, we have seen solutions where, by reducing the privacy level, digital tools have been used to help public health authorities contain the virus. But, can we have a more human, personalised, privacy-preserving approach to information, while still being able to contain the virus? Can we achieve individual privacy and still create a solution for public health? Well, it seems the answer is yes.

Decentralised, Citizen-Led, Community-Owned Data Collaborative

Our team, led by Ramesh Raskar, MIT Media Lab Associate Professor, has created a digital contact-tracing solution, “COVID SafePaths,” that does exactly that. The team is composed of a consortium of epidemiologists, engineers, data scientists, digital privacy evangelists, professors, and researchers from reputable institutions. It is a step towards acting efficiently around the problems we’re trying to solve, as well as reducing the vulnerability associated with holding on to sensitive data. It is a Collective Data intelligence Project rooted in a deep understanding of and respect for human needs of privacy and control.

Now, on the surface, this may seem very difficult because privacy is not just about an individual. There are other factors that play a role, such as consent, regulations like HIPAA, trade secrets between organizations, and, of course, national security. Some might say, “What is in it for me, what's the incentive?“ or “I'm already healthy. Why should I worry about a system like this?” There is also a possibility of an alternate view on privacy where location data might seem like low-stakes information. Some people would even make a favorable case for giving out anonymized and aggregated private data such as location. But we can see that de-identification aggregation is not at all enough. Consider the case of Strava, a popular app that people use for outdoor activities. It generates a Global Heatmap, relying completely on data contributed by athletes from all over the world. They released their anonymized and aggregated trails, but that ended up disclosing the outlines of U.S. military bases in Nigeria and Syria. So even what seems like low-stakes information, in this case GPS coordinates of athletes, could actually become a national security issue. This points out the vulnerability of using such an approach.

What about Bluetooth? It does seem like a safer option as it does not give away the location, but rather gives a proximity. But there is a challenge there as well. There are some widespread third-party apps that have hundreds, or even sometimes billions, of installations. They can start listening to all these Bluetooth beacons that are being emitted by these phones and can easily create the identifiable trajectories. So these are not easy problems to solve and we need to think about this in a computational way as well.



Multi-Fold Improvement in Contact-Tracing

COVID SafePaths, which is available now on the Google Play store and Apple app store as its beta PrivateKit, works like a digital diary. In this beta version, individuals can start logging personal trails in this diary on their own phone, without sharing any information with anyone. Then, they can download the data from public information to assess for themselves what the risks are. In version two, we expect public health authorities to start listing redacted location trails and Bluetooth trails of infected people. Redacted trails provide sufficient privacy for the infected person. For the benefit of everyone else who is healthy, individuals can download this data and look at the intersection on their own phones. But in version three, we would like to reduce the burden on health officials, who may have to do these personal interviews and redaction, by implementing computational methods to do semantic analysis, redaction, anonymization, aggregation, blurring, merging, and publishing.

Safe Paths, Yes. But we also need Safe Places!

For this to work effectively, we also are building SafePlaces, a web-tool for public health officials. Containment of an infectious disease requires identification and quarantine of infected individuals and potentially infected individuals. COVID SafePlaces helps health officials and epidemiologists work more quickly, collect better data, and watch and respond to what is happening in their community. With SafePlaces, at least in version one and version two, patients would need to donate their data on a consent basis to the app. Their data would be a 20- or 28-day trail of their GPS and Bluetooth contacts. The health officials can redact private information such as locations of home, where you work, or places that should not be marked as possible sites of exposure. For instance, if you just travel in your own car down the main street, we know that there is no need to mark all of that street as a red zone. Additional tools allow the public health official to anonymize, aggregate, merge, and use computational methods for data protection. COVID SafePlaces helps health officials and epidemiologists work more quickly, collect better data, and watch and respond to what is happening in their community. We are working with many cities currently in the U.S., as well as several countries worldwide, to deploy SafePlaces for public health officials in a way that complements the COVID SafePaths App for individuals. We have a decentralised approach that ensures that the right people have the right tools to manage or access relevant data and deliver the best social outcomes.

Humans Committed to Flattening the Curve

This project has grown into a wonderful alliance, which is open source and available on GitHub. We encourage people to participate in many ways. People around the world are working with us by contributing code, valuable contributions to our Think-Tank, or participating in the rollouts. The COVID SafePaths project is a multi-faculty, cross-MIT effort, with input and expertise from institutes including Harvard University, Stanford University, and the State University of New York at Buffalo; clinical input from Mayo Clinic and Massachusetts General Hospital; and mentors from the World Health Organization, the U.S. Department of Health and Human Services, and the Graduate Institute of International and Development Studies. Experts from government agencies and academic institutes in Canada, Germany, India, Italy, the United Kingdom, and Vietnam are also helping to guide the platform's development.

Need of the Hour: Reassurance & Equitable Resilience

If we have tools to orchestrate and coordinate amongst citizens, it's not just about public health. If we have enough privacy guarantees in the short run, we will be able to overcome the challenges of slowing the spread of the virus. But in the medium term, such orchestration tools will also allow us to restart the economy.

And eventually our goal is to create resilient societies that can overcome these challenges presented by human made and natural disruptions to our social and economic fabric. Data is fundamental to our situational awareness and response to such epidemics. The mining of such data informs the design and implementation of services. Adoption of a solution like COVID SafePaths and SafePlaces will trigger a change in the way we capture, visualise, and communicate data. What we need for the society to move forward is a trusted, impartial, honest broker who has an all-seeing, all-knowing view of what is going on, but not through a "big brother" surveillance system – instead a system that is benevolent. Through a collaborative ecosystem with a privacy-first approach like this one, we would be able to optimize for individual, communal, and societal outcomes, where data becomes an asset that positively impacts us all.