Covid19 Contact Tracing: Overview MIT Technology Review

Marija Gojković, Milan Ilić

Introduction

MIT (Massachusetts Institute of Technology) Technology Review is a magazine which originates from MIT University, intending to promote new technologies and commercialize it [1]**.** This brief paper aims to provide the Overview of Magazine's articles concerning the Covid-19 Contact Tracing topic.

Contact tracing—tracking who has a disease and who those people have been near in order to limit the spread of an outbreak—is a crucial tool in fighting diseases, including covid-19 [2].

The issue of privacy and trust

One of the most used technology is the software that Apple and Google jointly built into iPhone and Android devices to help track the spread of coronavirus by telling users if they contacted an infected person and are potentially sick themselves.

Contact tracing technique has been one key to the success of countries like South Korea in turning back the tide of the pandemic inside their own borders. Crucially, Apple – Google app isn't the national coronavirus surveillance system and the system's implementation will vary from country to country with the availability only to government public health agencies directly involved in coronavirus tracking.

This contact tracing network, relies on Bluetooth, typically used for short-distance communication between devices. When you test positive for the virus, you enter that information into an app on your phone, and other people who have been near you in the previous 14 days are alerted. Your own information remains private.

But one of the biggest issues that arise is the issue of privacy and trust. Are they going to be concerned that this surveillance system—after all, contact tracing is ultimately a form of surveillance—will come back to haunt them [2]?

In China, an authoritarian regime with a long history of maximalist surveillance, required citizens to an app that dictated whether they would be quarantined or allowed to move freely; the data is shared with police. In South Korea, a democracy that was the scene of early outbreaks, a pandemic surveillance system allowed the government to access smartphone location, credit card histories, immigration records, and CCTV footage from around the country. Taiwan has built "electronic fences" that track location to make sure that people are staying in place during quarantine. These systems may work, but they are also profoundly invasive.

Apple and Google say they are helping government public health agencies in North America, Europe, and Asia build their own apps that utilize the same underlying technology. Those governments will have their own rules, but the app will require explicit user consent to start tracking, and the user can always turn it off—either permanently or temporarily. Importantly, the new system doesn't collect any true location data: it's all proximity data gathered by Bluetooth. This means the system will know that you and another person at one point crossed paths for some amount of time, but that information won't leave your phone until you choose to share it—and when you do, neither Google, Apple, nor other users will learn their identities or medical status. And the matching is only

done on-device, the companies say. There is no single centralized server, though health organizations will be part of a decentralized infrastructure running the system. The aim of decentralization is to make malicious surveillance immensely difficult. Additionally, while each country's public health authority will build its own app using the Google-Apple system, the two companies say they will shut it down on a region-by-region basis when the pandemic is over.

Project: Covid Tracing Tracker

As the covid-19 pandemic rages, technologists everywhere have been rushing to build apps, services, and systems for contact tracing: identifying and notifying all those who come in contact with a carrier. Some are lightweight and temporary, while others are pervasive and invasive. So to help monitor this fast-evolving situation, authors of the Magazine gathered the information into a single place for the first time with their Covid Tracing Tracker—a database to capture details of every significant automated contact tracing effort around the world [3].

At the most basic level, database compiles a list of automated contact tracing apps that are backed by national governments. For each newfound app, there are basic questions asked:

- **Is it voluntary?** In some cases, apps are opt-in—but in other places many or all citizens are compelled to download and use them.
- **Are there limitations on how the data gets used?** Data may sometimes be used for purposes other than public health, such as law enforcement—and that may last longer than covid-19.
- **Will data be destroyed after a period of time?** The data the apps collect should not last forever. If it is automatically deleted in a reasonable amount of time (usually a maximum of around 30 days) or the app allows users to manually delete their own data, we award a star.
- **Is data collection minimized?** Does the app collect only the information it needs to do what it says?
- **Is the effort transparent?** Transparency can take the form of clear, publicly available policies and design, an open-source code base, or all of these.

For each question, if the answer is yes , the app gets rated with a star in this database. If the answer is not yes—either because the answer is negative or because it is unknown—the rating is left blank.

Overview of used technologies

- **Location:** Some apps identify a person's contacts by tracking the phone's movements (for instance, using GPS or triangulation from nearby cell towers) and looking for other phones that have spent time in the same location.
- **Bluetooth:** Some systems use "proximity tracking," in which phones swap encrypted tokens with any other nearby phones over Bluetooth. It is easier to anonymize and generally considered better for privacy than location tracking.
- **Google/Apple**: Many apps will rely on the joint API that Apple and Google are developing. It lets iOS and Android phones communicate with each other over Bluetooth, allowing developers to build a contact tracing app that will work for both. Later the two companies plan to build this directly into their operating systems.
- **DP-3T**: This stands for decentralized privacy-preserving proximity tracing. It's an open-source protocol for Bluetooth-based tracking in which an individual phone's contact logs are only stored locally, so no central authority can know who has been exposed.

Some of the highest ranked apps used in different countries:

Austria: Stopp Corona

Austria was one of the first major European nations to align with the Google/Apple API [4], ranked with 5 ★ and using Bluetooth, Google/Apple technology.

Iceland: Rakning C-19

Iceland decided not to use Bluetooth [5] because it was too unreliable and instead uses location data, ranked with 5 ★, uses Location as technology.

Switzerland: SwissCovid

Initially, the Swiss opted to use DP-3T instead of the Google/Apple API. Now it looks they will be using both [6]. Ranked with 5 ★.

Apps using Apple – Google software

Bluetooth

Bluetooth is the chosen solution for most contact tracing because it's a low-power signal that's present in most phones, is highly resistant to blockage, and can be used in a way that preserves privacy. As part of its normal operation, it can measure the strength of a signal from another phone (known as the RSSI, or received signal strength indicator). In theory, the amount of power is proportional to distance, so it can be used to gauge how far the two phones are from one another. A strong signal means proximity; a weak one means the phones are further apart. Thus, a certain signal strength between two phones can indicate a "contact event" between their owners.

However, many things can mess that signal up and make the data incorrect. Things like walls, human bodies, pockets, or even proximity to several phones at once can throw the measurements off. One problem is that such a system could yield many false positives. If you are in the wide open, yours Bluetooth and other Bluetooth might ping each other even if you're much more than six feet (2 m approximately) away. You could be through the wall from me in an apartment, and it could ping that we're having a proximity event. You could be on a different floor of the building and it could ping. You could be biking by me in the open air and it could ping.

There are many other potential sources of error. For example, if your phone is standing up in your pocket—in portrait rather than landscape mode—it can significantly change the amount of received power. That alone can make it look as if somebody across the room is just a couple of feet from you [7].

IMPACT

However, the situation can be improved by taking more data into account and learning more about how to properly interpret signals. It's not at all hopeless, there are other sensors on our phones as well. For example, the ambient light sensor could tell you if your phone is in your pocket or purse, which tells you about potential blockages. Your accelerometers help; your compass and gyroscope can tell you how a device is oriented on multiple planes.

Jennifer Watson, a researcher at MIT's Lincoln Laboratory, has led a project where team members in quarantine measured in their own homes how variables like location, phone orientation, other phones, indicators of outdoor versus indoor, and various materials can affect signals. "There is enormous variability in received signals," she said. "What we wanted to do is get a handle on this very quickly in a simple way".

This paper [8] describes a method and analysis of determining whether two cell phones, carried by humans, were in persistent contact of no more than 6 feet over 15 minutes using Bluetooth Low Energy signals. The paper describes the approach to detecting these signals, as well as a data-driven performance analysis showing that larger numbers of samples with more optimal detection algorithms, coupled with privacy preserving auxiliary information, improves detection performance. Bluetooth Low Energy (BLE) beacons have been proposed as a method for accomplishing this detector, but it has many impediments to accurately distinguishing between contacts that are truly "too close" (as defined by the CDC) from those that are actually "too far".

However, with some feasible augmentations, authors of the paper believe a detector with superior performance (greater than 60% correct identification of true TCFTL events, with an FDR of 50%) can be constructed.

The Apple – Google API

For now, the software simply consists of an API (application programming interface) that lets Apple and Android phones, which use distinct operating systems, swap data with each other. Users have to separately download apps created by health authorities that use the API as the underlying system for exchanging data. The data will be accessible to public health officials but will not include information that is personally identifiable either to the companies or to governments. Later on, the two firms plan to add contact -tracing software directly into the operating systems, so that it will be on more people's phones by default [9].

Exposure notification

The Exposure Notification Service is the vehicle for implementing exposure notification and uses the Bluetooth Low Energy wireless technology for proximity detection of nearby smartphones, and for the data exchange mechanism [10].

- **Temporary Exposure Key** — A key that's generated every 24 hours for privacy consideration.
- **Diagnosis Key** — The subset of Temporary Exposure Keys uploaded when the device owner is diagnosed as positive for the coronavirus.
- **Rolling Proximity Identifier** — A privacy preserving identifier derived from the Temporary Exposure Key and sent in the broadcast of the Bluetooth payload. The identifier changes about every 15 minutes to prevent wireless tracking of the device.
- **Associated Encrypted Metadata (AEM)** — A privacy preserving encrypted metadata that shall be used to carry protocol versioning and transmit (Tx) power for better distance approximation. The Associated Encrypted Metadata changes about every 15 minutes, at the same cadence as the Rolling Proximity Identifier, to prevent wireless tracking of the device.

Maintaining user privacy is an essential requirement in the design of this specification. The protocol maintains privacy by the following means:

- The Exposure Notification Bluetooth Specification does not use location for proximity detection. It strictly uses Bluetooth beaconing to detect proximity.
- A user's Rolling Proximity Identifier changes on average every 15 minutes, and needs the Temporary Exposure Key to
- be correlated to a contact. This behavior reduces the risk of privacy loss from broadcasting the identifiers.
- Proximity identifiers obtained from other devices are processed exclusively on device.
- Users decide whether to contribute to exposure notification.

- If diagnosed with COVID-19, users must provide their consent to share Diagnosis Keys with the server.
- Users have transparency into their participation in exposure notification.

References

[1] MIT_Technology_Review: en.wikipedia.org/wiki/MIT_Technology_Review

[2] How Apple and Google are tackling their covid privacy problem: www.technologyreview.com/2020/04/14/999472/how-apple-and-google-are-tackling-their-covid-privacy-problem

[3] Covid Tracing Tracker: www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker

[4] Stopp Corona app: www.stopp-corona.at

[5] Rakning C-19 app: www.covid.is/app/is

[6] Swiss-covid app: foph-coronavirus.ch/swisscovid-app/#download

[7] Bluetooth contact tracing needs bigger, better data: www.technologyreview.com/2020/04/22/1000353/bluetooth-contact-tracing-needs-bigger-better-data

[8] PACT: Private Automated Contact Tracing (MIT) pact.mit.edu/wp-content/uploads/2020/11/TCFTL_paper_FINAL_V15_w_logos.pdf

[9] Bluetooth API Apple - Google www.bag.admin.ch/dam/bag/en/dokumente/cc/kom/covid-19-faq-tracing-app-einsatz-bluetooth-api-apple-google.pdf.download.pdf

[10] Exposure Notification – Bluetooth Specification: covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf