Decentralized Privacy-Preserving Proximity Tracing: Simplified Overview

based on version: 3rd April 2020 – non authoritative version

3rd April 2020. For more information and authors, see the full white paper.

Disclaimer/Provenance

This document is a manually created, LaTeX version, of the original document at https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf as as captured on 2020-04-08. As this document was only available as a PDF it was hard to collaborate in typical Open Source style.

This *non-authoritative, derived*, version is to facilitate easier edits/contributions and collaboration.

See https://github.com/DP-3T/ for the correct versions.

Decentralized Privacy-Preserving Proximity Tracing: Simplified Overview

based on version: 3rd April 2020 – non authoritative version

3rd April 2020. For more information and authors, see the full white paper.

There is growing political and epidemiological interest in deploying technological approaches to help individuals and countries navigate the COVID-19 pandemic. One approach has been to make use of low-powered Bluetooth sensors on smartphones to inform users when they have been in contact with individuals who have since tested positive, and to support epidemiologists with modelling efforts. However, not all proposed infrastructures that can enable proportionate proximity tracing are the same. Some of these proposals may fail to protect data, or be misused or extended far beyond their initial purpose and beyond the lifetime of the crisis. This is all the more important given the truly global nature of this challenge and the fact that the pandemic crosses across borders and jurisdictions with different levels of fundamental rights guarantees and in times where many governments are functioning under rules of exception.

We currently see different approaches emerge across countries and groups:

- **Data grab model**: Suggesting that due to exceptional conditions it is legitimate to obtain location, telecoms, sensor data collecting in existing commercial and public infrastructures, centralise it and analyse it, relying on legal norms to protect these efforts. This model advocates disproportionate collection of personal data, and assumes legal protections will be sufficient to protect populations which are often not the case.
- **'Anonymised' data approach**: Solutions that propose to anonymise existing location, telecoms sensor data for further use in the pandemic. Anonymisation of personal data is a difficult, if not impossible bar to reach. For location data, for example, this will generally be 'privacy washing', as such rich data is impossible to effectively anonymise. Such solutions also lack in purpose specification and proportionality.
- **Designs to minimise data collection**: Solutions that propose setting up an infrastructure specific to collecting only data needed for fulfilling proximity tracing needs of health authorities or epidemiologists. Proposals avoid relying on data collected by existing commercial or public infrastructures that were not set up for the goal of proximity tracing. These solutions can range between centralized and decentralized models:
  - **Centralized** models attempt to minimise data by generating and keeping track of ephemeral identifiers distributed to users which can be used to construct the contact graph of a user only in the case they are infected. The generation of identifiers and generation of contact graphs are done on a server which is often assumed to be controlled by a government or another trusted entity. This model assumes that the entity running the server shall not misuse the data and capabilities of the server other than when people

are infected, for example, at the request of law enforcement, border control or intelligence agencies. Such protection relies on the protection of the central server which can potentially be repurposed into a 'data grab' model.

– **Decentralized** models are designed to keep as much sensitive data on users devices as possible. Methods are introduced to strictly control data flows in order to avoid accumulating any contact data on a centralized server. This means that a server exists but only to enable people to use their own devices to trace contacts. The server is not trusted with sensitive data at all and therefore is not vulnerable to function creep like all the other solutions.

Given the concerns around the effectiveness of legal measures, the impossibility of anonymization, and the intrinsic vulnerabilities of centralized data minimization models, we focus on a decentralized design for privacy preserving proximity tracing. As discussed above, designs with centralized proposals raise concerns: if they are attacked, compromised or repurposed, they can generate great harm and broadly so. **In order to mitigate these issues, we implement proximity tracing using a decentralized design that does not require the centralized collection and processing of information on users**. Such a design builds in strong, mathematically provable support for privacy and data protection goals, minimises the data required to what is necessary for the tasks envisaged, and prevents function creep, for example for law enforcement or intelligence purposes, by strictly limiting how the system can be repurposed through the application of cryptographic methods.

The decentralized system works in 4 phases:

1. **Installation**: the app is installed, generates a secret piece of data it uses to derive a chain of identifiers to broadcast out.
2. **Normal operation**: each app broadcasts ephemeral identifiers via bluetooth, and records ephemeral identifiers that are broadcast by other apps in the vicinity. The app rotates the broadcasted identifiers frequently. A third-party listening out will not be able to predict the next one that is rotated to, and so cannot use this to track individuals (e.g. to spot repeat visits to the same place).
3. **Handling infected patients**: after patients are diagnosed, and only with their consent and with authorization from a health authority, they (with an authorisation code) upload data from their phone to the backend server, from which the last 14 days of the identifiers they broadcast can be recreated. From this data, the identity of the patient cannot be derived by the server or by the apps of other users, it is in effect anonymous.
4. **Decentralized contact tracing**: each app can use the data they download from the backend to compute privately on their own device whether the app's user was in physical proximity of an infected person and potentially at risk of infection. If they were, the app can inform the user to take action.

Additionally, app users can *voluntarily* provide (anonymous) data to epidemiology research centers.

This system:

- **Ensures data minimization**. The central server only observes anonymous identifiers of infected people without any proximity information; health authorities learn no information (beyond when a user manually reaches out to them after being notified); and the epidemiologists obtain an anonymized proximity graph with minimal information.
- **Prevents abuse of data**. As the different entities in the system receive the minimum amount of information tailored to their requirements, none of them can abuse the data for other purposes, nor can they be coerced or subpoenaed to make other data available.
- **Prevents tracking of non-infected users**. No entity, including the backend server, can track non-infected users based on broadcasted ephemeral identifiers.
- **Graceful dismantling**. The system will organically dismantle itself after the end of the epidemic. Infected patients will stop uploading their data to the central server, and people will stop using the app. Data on the server is removed after 14 days.

Avoiding the accumulation of sensitive data on a centralised database comes at the 'cost' of localized vulnerabilities elsewhere in the infrastructure. Specifically, we see two types of high-effort attacks on the system which are theoretically possible.

- A tech-savvy adversary could reidentify identifiers from infected people that *they have been physically close to in the past by* i) actively modifying the app to record more specific identifier data and ii) collecting extra information about identities through additional means, such as a surveillance camera to record and identify the individuals. This would generally be illegal, would be spatially limited, and high effort.
- A *tech-savvy* adversary deploying an antenna to eavesdrop on Bluetooth connections can learn which connections correspond to infected people, and then can estimate the percentage of infected people in a small radius of 50m.

Our protocol is demonstrative of the fact that privacy-preserving approaches to proximity tracing are possible, and that countries or organisations do not need to accept methods that support risk and misuse. Where the law requires strict necessity and proportionality, and societal support is behind proximity tracing, this decentralized design provides an abuse-resistant way to carry it out.

3 April 2020

Contact author: Prof. Carmela Troncoso, EPFL