MIT Computational Law Report

COVID-19 Contact Tracing Privacy Principles

Dazza Greenwood, Gregory Nadeau, Pagona Tsormpatzoudi, Bryan Wilson, Jeffrey Saviano, Alex "Sandy" Pentland

Published on: Apr 06, 2020

Updated on: May 20, 2020

License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)

Use this Google Form to offer additions and corrections to this working draft contact tracing privacy principles or to offer other contributions to the upcoming Special Release on COVID-19 Legal Frameworks.

This working draft document is for rapid input in support of an upcoming Special Release on COVID-19 Legal Frameworks to be published as part of the MIT Computational Law Report at Law.MIT.edu. An editorial and research tiger team are actively collecting and curating privacy principles for COVID-19 contact tracing applications and services that leverage personal individual location and proximity data.

Please note, we have also included materials from other groups on contact tracing privacy principles, potentially to synthesize into an overall set of principles.

law.MIT.edu Working Draft: Contact Tracing Privacy Principles

> *Version 0.2 - April 30, 2020*

Lawful

Contact tracing apps must comply with all applicable laws, rules and regulations. Any data collection and use must have a lawful basis.

Informed Consent

A user must provide informed consent as a prerequisite for installation and use of a contact tracing app. A user should be able to give their consent to each functionality of an app separately, such as collection of proximity data, location data, sharing data or other key separate functions.

Identity Control

Users make the determination to release redacted, disconnected, and/or aggregated space-time points from location data, or obfuscated identifiers from e.g.,Bluetooth.

Space-time points should be deleted after they are no longer actively needed, estimated at between 21 and 28 days.

No information about an at-risk user should be required other than that which is essential, based on epidemiological standards, for alerting others to potential exposure.

Aggregate data may be maintained for public research purposes. Precautions should be taken to ensure that shared aggregate data may not be re-identified downstream.

Users must be able to view and have a copy of the data collected about them and also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the user.

Transparency

Users should be given notice of an organization's information practices before any personal information is collected from them. Organizations should explicitly describe the following:

- identification of the entity collecting the data;
- identification of the uses to which the data will be put;
- identification of any potential recipients of the data;
- the nature of the data collected and the means by which it is collected;
- whether the provision of the requested data is voluntary or required;
- the steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data.

Contact tracing apps should use open source code and publicly vetted cryptographic algorithms. Contact tracing apps should use an openly published protocol to ensure that their solution is verifiable and interoperable. For example, DP^3T, PACT, the TCN Protocol, and Apple/Google COVID-19 contact tracing technology.

Accountability

In order to ensure that organizations adhere to contact tracing privacy principles, there must be enforcement measures, such as: Self-regulation by the information collectors or an appointed regulatory body; Private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and Government enforcement that can include civil and criminal penalties levied by the government.

Relevant stakeholders should be fully involved and consulted in the development and deployment of a contact tracing app, including data protection authorities, the privacy and security community, human rights and civil liberties organizations, government agencies, technology community, and public health professionals, including epidemiologists.

Proportionality

The potential risk that private information may be exposed or misused as a result of a contact tracing system must be proportional to the public health benefits of that system for combating the epidemic.

The analysis of proportionality should take into account the efficacy of the contact tracing app at reducing the incidence of new cases and factors including but not limited to scope and purpose of the contact tracing app, type(s) of data collected, collection processes, sharing, retention, and deletion of data.

Other Pillars

This document addresses privacy principles as a key pillar supporting successful contact tracing systems, however this is not the only pillar. The following are other pillars that are related to privacy but discernible from and beyond the scope of privacy principles.

Voluntary

Use of contact tracing apps should be voluntary and not mandatory or compelled.

Trustworthy Criteria of Aggregate Data Holders

Data may be aggregated so that it may not allow for the identification of individuals. Aggregate data should be processed with privacy-protecting techniques such as differential privacy. The methodologies and techniques should be available for public review. Aggregate data may be maintained for public research purposes. Precautions should be taken to ensure that shared aggregate data may not be re-identified downstream.

In a system that includes an aggregate data holder, the capabilities, duties and motivations of such entity must be appropriate to its responsibility to safeguard the rights of people whose data it holds. Ideally, such entity would hold fiduciary obligations to the people whose data it holds, but other combinations of requirements, constraints, incentives and counter-incentives can perform the same function.

Security

Information collectors should ensure that the data they collect is accurate and secure. They can improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors can keep their data secure by protecting against both internal and external security threats. They can limit access within their company to only necessary employees to protect against internal threats, and they can use encryption and other computer-based security systems to stop outside threats.

Effectiveness

The basic prerequisite is that “contact tracing” can realistically help to significantly and demonstrably reduce the number of infections. The validation of this assessment is the responsibility of epidemiology. If it turns out that “contact tracing” via app is not useful or does not fulfill the purpose, the experiment must be terminated. The application and any data collected must be used exclusively to combat SARS-CoV-2 infection chains. Any other use must be technically prevented as far as possible and legally prohibited.

The effectiveness at combating the SARS-CoV-2 infection should be established based on objective, measurable criteria and professional assessment or evaluation practices, such as auditing and testing

regimes.

Usability

Contact Tracing apps must be fully accessible and based on the latest W3C/WAI standards.

Equity

Contact Tracing apps shall be developed in collaboration with the privacy and security community, human rights and civil liberties organizations, government agencies, technology community, and public health professionals, including epidemiologists.

Commentary

[Drafting commentary for each principle is currently in progress and will be released as part of Version 0.3 of these Privacy Principles]

Privacy Adherence Assessment

[The Privacy Adherence Assessment is currently in progress and will be released as Version 0.4 of these Privacy Principles]

Research

Contact Tracing Privacy Principles: Clause-level Overview

Background Materials

Co-Epi: Contact Tracing Bill of Rights

Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask

10 requirements for the evaluation of “Contact Tracing” apps

Data Rights for Digital Contact Tracing and Alerting · Overview

Data Rights for Exposure Notification - Overview

EU Guidance for Contact Tracing Apps

ACLU White Paper: The Limits of Location Tracking in an Epidemic

EFF: The Challenge of Proximity Apps For COVID-19 Contact Tracing

Data Protection in Telemedicine

Use this Google Form to offer additions and corrections to this page or other contributions to the upcoming Special Release.