MIT Computational Law Report

Commentary on COVID-19 Contact Tracing Privacy Principles

Dazza Greenwood, Bryan Wilson, Ryan Carrier, Mark Potkewitz, Ajintha Pathmanathan, Nadia Diakun-Thibault, Cari Spivack, Matt Gee, Nishant Bhajaria, Kelsey Finch, Pagona Tsormpatzoudi, Jonathan Askin, Tony Lai

Published on: Aug 14, 2020

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

> *This work follows up on the MIT Computational Law Report's Contact Tracing Privacy Principles, an on-going initiative that was first published in the Spring.*

0. Introduction

Over the last several months, the MIT Computational Law Report has convened a weekly series of working meetings to collect, evaluate, and curate privacy principles for contact tracing applications and other services that leverage individual location and proximity data to combat COVID-19. These working meetings have included a diverse group of stakeholders with backgrounds in law, technology, epidemiology, from the public sector, the private sector, government, and academia. While the initial set of principles were well received[1] and served their purpose in providing essential guidance about *what* the privacy principles for these sorts of applications ought to be, this document and accompanying video explores *why* we decided on this set of privacy principles and the implications therein.

Visit the web version of this article to view interactive content.

Commentary Panel on MIT Contact Tracing Privacy Principles

The remainder of the document includes 1. a set of definitions, 2. an overview of each of our principles with commentary about why each principle was selected and identification of issues that are important to resolve, and 3. an overview of some of the additional pillars, beyond privacy, that necessarily play a role in the discussion of contact tracing applications.

1. Definitions

The definitions we have included in this section include some of the most popular terms that are used within the context of contact tracing.[2] This list is not exhaustive and is primarily intended as a way to provide a foundation for some of the discussion later on in this article.

Anonymized Personal Data

The process of creating Anonymized Personal Data, or anonymization, is a direct attempt to hide the identity of any individual by combining them into an aggregate without the need for individual or specific references.

Aggregate Data

Refers to data that is collected in accordance with a specified process and that has specific safeguards in place in order to ensure that the data will not be used to re-identify any individual record. For example "Aggregate data meta-analysis (ADMA) combines the grouped data of primary studies,

whereas individual patient data meta-analysis (IPDMA) synthesizes the individual data of primary studies."[3]

Authority

Authority broadly refers to those groups with the authorization to conduct digital contact tracing. It is important to consider that different authorities operate at different levels. Authority can include global authorities, such as the World Health Organization. Authority can also include national authorities, such as the Center for Disease Control and the National Health Service. Authority can also include those local public health authorities and other Contact Tracing Entities who are directly interfacing with patients who have been diagnosed with COVID-19 and those suspected of having contracted COVID-19. Authority can also include private parties who are contractually obligated to conduct contact tracing, such as in the employer-employee context.

Centralized

The Contact Tracing Entity has sole authority for collecting the contact tracing data and deposits it in a singular location.

Consent

Consent of the contact tracing subject means any freely given, specific, informed and unambiguous indication of the subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her for the purpose of contact tracing.[4]

Contact Tracers

A person or machine who will, among other things, interview those who receive a positive test result in an attempt to identify and inform other individuals who have been deemed to be in close enough proximity to be considered at-risk.

Contact Tracing

Contact tracing is the process of identification of persons who may have come into contact with an infected person and subsequent collection of further information about these contacts.

Contact Tracing Entity

An Authority having power or control to conduct a contact tracing program.

Contact Tracking

The act of using a contact tracing system to monitor and/or enforce quarantine or restrict movements once a positive test has been medically verified.

De-Anonymization

The practice of deliberately processing aggregate anonymized data for the purposes of re-identifying individual persons specifically regardless of the rationale or merit. De-Anonymization does not include security tests which are designed with the knowledge of the owner and anonymizer of the aggregate data to verify the quality and security of the anonymization process.

De-Identification

De-identification refers to the process of removal of identifying information from a dataset so that individual data cannot be linked with specific individuals.[5]

Deletion

Deletion means eradication of all data stored and associated with a deletion request, whether identified as a MAC address, IP, or other protocol which matches the identity of the request or requirement. Primary data refers to the locations of current usage for data, where all applications and algorithms connect to the data for usage and reference.

All backup data, which refers to the location where data is replicated or stored for the purpose of replacing Primary Data, must be tagged with a unique ID, called a RESTOREID, which connects the Primary Database with the Backup Database. All references and links must be erased and delinked from the Primary Data storage location and the RESTOREID that connects to the Backup Data must be eradicated. Failure to eradicate the RESTOREID should result in a breach of deletion criteria.

All retrieval of data from a Backup Dataset must validate the RESTOREID – failure to validate means that a deletion event has occurred, and thus, the Backup Data must be destroyed and may not be called up for restoration.

Article 17 of the GDPR includes an important provision requiring deletion of personal data at the request of the person identified.

Digital

Characterized by electronic and especially computerized technology.

Digital Handshakes

The connections made between two Contact Tracing technology devices which record data.

Exposure Notification

A successful notification of exposure allows for an exchange of information with and exposed person (contact) and offers an opportunity to answer questions and provide referrals for testing, medical

evaluation and other necessary support services.[6] The goals of this interaction are to inform the person that they may have been exposed, assess their medical condition and other risk factors, and gather information for continued monitoring and support.[7]

Guardian

A person who has the legal authority to act on behalf of another.

Independent Governance

Independent means not influenced or controlled by others in matters of opinion, conduct, etc.; thinking or acting for oneself. Members of the governance body must not be affiliated with the entity providing the tracing systems. Further, if the government is the implementing authority, the independent panel should represent the people and have the means to be transparent, hear from and interact with the people. Governance means supervision; watchful care and the authority to call for change.

Jurisdiction

The legal region or geography in which a contact tracing program may be conducted.

Mandated

Mandated means that the authority or even technology provider leaves no choice to the user.

Network Provider

Entity which delivers the signal between a device and the database, or the database and the Contact Tracer.

Non-essential, Contracted

Entity which does not require data, personal data, or sensitive personal data to execute their contractual role in the Contact Tracing program.

Opt-in

Opt-in refers to taking some action to expressly indicate consent. Opt-in privacy policy frameworks offer the characteristic of individual choice free from coercion.

Opt-out

Opt-out refers to taking some action to expressly revoke consent. Opt-out privacy policy frameworks, in their application, are more coercive in nature than opt-in policies.

Personal Data

Personal data, also known as personal information, or personally identifiable information is any information relating to an identifiable person.

Public Health Emergency

A "public health emergency" is an occurrence or imminent threat of an illness or health condition that: (1) is believed to be caused by any of the following: (i) bioterrorism; (ii) the appearance of a novel or previously controlled or eradicated infectious agent or biological toxin; (iii) [a natural disaster]; (iv) [a chemical attack or accidental release; or] (v) [a nuclear attack or incident]; and (2) poses a high probability of any of the following harms: (i) a large number of deaths in the affected population; (ii) a large number of serious or long-term disabilities in the affected population; or (iii) widespread exposure to an infectious or toxic agent that poses a significant risk of substantial future harm to a large number of people in the affected population.[8]

Publicly

As an adjective, open to all; notorious. Open to common use. Belonging to the people at large; relating to or affecting the whole people of a state, nation, or community; not limited or restricted to any particular class of the community.

Registration

The first step acceptance and process to join the technology of an opt-in contact tracing system.

Regulation

Broadly speaking, several jurisdictions differentiate between *statutes* (see below) and *regulations*. The term "regulation" typically refers to a rule imposed by some sort of agency or regulatory body that comes with the threat of some legal penalty of civil sanction but remains separate from a *law* or *statute* since regulations are not passed by a legislative body. Agencies often impose regulations over industries or subject areas in response to laws authorizing or compelling those agencies to establish and impose regulations to address concerns of the legislative body.

Sensitive Personal Data

Definition under the GDPR: data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.[9]

Service Provider

A third-party technology provider who is supplying critical infrastructure and services to the Contact Tracing technology.

Start Date

The day and time at which a contact tracing program is initiated.

Statute

A statute or law refers to a rule or set of rules passed by a legislative body through a legitimate process and promulgated that seeks to regulate the behavior of people in a given society and threatens criminal penalty or civil sanction for violations or non-compliance.

Third Party Doctrine

In the United States, the "Third Party Doctrine" refers to the judicial holding that information deliberately and knowingly shared with a third party loses the constitutional expectation of privacy created by the Fourth Amendment to the U.S. Constitution.[10] Many people incorrectly believe that government agencies need judicial warrants to compel companies to turn over an individual's data for the purposes of an investigation. However, many types of information or records fall within this "third-party doctrine" exception. As a general rule, nearly *any* information exposed to a third party falls within this exception. For example, when I place a phone call, I am presumed to understand that I am necessarily sharing certain information with both the person I'm calling *and* the telephone company. While the *content* of the call remains protected, the fact that a call took place, the time the call began, the time the call ended, the number of the originating call. US courts have found that certain sorts of information such as telephone records,[11] banking and financial records,[12] as well as to/from and other non-content-related email data[13] do not have the protection of the Fourth Amendment.

Underaged

A natural person who has not reached the minimum age required either law or program criteria for the contact tracing program.

2. Principles

These principles were iteratively developed based on the feedback from a large number of people. Our preliminary approach was to identify existing privacy principles, break them down into individual clauses or bullet points, enter them into a spreadsheet, and group them by principle, keywords, etc. We looked at work developed by other groups, including CoEpi & CovidWatch,[14] the Computational Privacy Group,[15] the Chaos Computer Club,[16] and the U.S. Digital Response,[17]as well as guidance on

contact tracing and exposure notification from the European Commission,[18] the Electronic Frontier Foundation,[19] the American Civil Liberties Union,[20] the Brookings Institution,[21] Harvard's Berkman Klein Center for Internet & Society,[22] and John Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies.[23] In the weeks that followed this initial dive, we crafted v 0.1 and v 0.2 of these principles, which reflected substantial feedback from the authors listed, and additional feedback from epidemiologists, regulators, data governance experts, privacy advocates, and technologists. The section proceeds by listing each principle and then summarizing some of the thinking and background behind why we chose the language that was included in the previous version.

Lawful

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

Lawfulness means that a law or regulation permits the collection, use, and sharing of data. The legal basis should directly correlate to the use of this data for the purpose of making a significant impact against the pandemic. Lawfulness further ensures that all persons, institutions, and entities that deploy contact tracing applications are accountable to the rule of law.

The reason we chose this language and we put this principle first is because lawfulness undergirds contact tracing and especially digital contact tracing. In some countries, the authority to conduct contact tracing is directly vested in power granted to the government. In other countries, this authority is assumed within broader regulatory frameworks or left alone to private lawfulness created through the terms of service of private vendors. Contact tracing and contact tracing applications will meet the lawfulness threshold when implemented by a state under statute or regulation, when implemented by private parties (e.g., under contract or permitted employee rules, in private schools, etc.).

As a practical matter, many issues can arise out of the way the legal basis for digital contact tracing apps is established. In some cases, such as under the GDPR, there will be requirements of private companies to certify that user data that is being collected by a contact tracing app is meeting certain thresholds and requirements. Another practical issue for consideration comes from understanding how different governments are using information that is collected by digital contact tracing apps. Is the right information being collected? Is it being stored properly? Is it being deleted within the timeframe specified by an existing law? These are all issues that could well be resolved by requiring independent audits of those parties that are associated with contact tracing apps. Finally, because the pandemic is specifically focused to the specific purpose of a disease that will, at some point, be substantially mitigated, it is quite important that the legal basis of contact tracing apps be limited to the pandemic itself. For governments, this can be accomplished by introducing sunset regulations.

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 grant consent to each functionality of an app separately, such as collection of proximity data, location data, sharing data or other key separate functions.*

As technologies have become more advanced and abstracted from the original conception of informed consent, so have the analogies used to evaluate them. With this in mind, developers of digital contact tracing apps should offer users the opportunity to provide consent, revoke consent, or refresh consent any time a material change from the initial circumstance when consent was given. These can include, but are not limited to, updates to the application, changes to legal authority (e.g., when a person enters into a new jurisdiction), new knowledge about the spread of COVID-19 being revealed, etc.

We believe the standard for consent should be elevated to always be informed, in accordance with the definition of GDPR, which we use above: consent of the contact tracing subject means any freely given, specific, informed, and unambiguous indication of the subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her for the purpose of contact tracing.[24] This means consent needs to be addressed throughout the lifecycle of contact tracing and all of the foreseeable circumstances during which new consent may be required.

Because digital contact tracing can involve multiple technologies for different aspects of the contact tracing supply chain, it is important to acknowledge that informed consent will also manifest in different ways. For example, a public health authority conducting an interview with an infected person over the phone and using a digital contact tracing app will need to obtain informed consent in a different way than a public health authority conducting an in-person interview with an infected patient. While these differences do exist, we recommend that both app providers and public health authorities create guidelines that are clearly updated, that can be audited and accounted for, and that empower users to make the decisions that are best for themselves.

Right to 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. The duration after which information should be deleted should be virus-specific and related to the latest scientific evidence.*
>
> *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 receive 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.*

Initially, this principle was labeled "Identity Control" and was later updated to "Right to Control" in order to recognize a broader, more accurate array of possibilities for an individual's ability to control data. Right to Control is intended to cover the need for data minimization and, generally, fair information practices.[25] These items are consolidated in order to achieve a relatively succinct high level set of principles and expounded upon below.

Technique	***Overview***	***Effectiveness***
Pseudonymization	Pseudonymization is a method to substitute identifiable data with a reversible, consistent value.	Low
De-identification	De-identified information means information that can not reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual, household, or device. De-identification is focused on an example for a single individual to be identified from specific connections between the descriptors, an example would be the introduction of an image, token or icon to replace first, last or full name.	Middle
Anonymization	Anonymization is a direct attempt to hide the identity of any individual by combining them into an aggregate without the need for individual or specific references.	Highest

Right to control also applies to 2nd and 3rd-order data identifiers, which machine learning or deep learning techniques might try to attach to an individual. For instance, a 2nd-order identifier might be location or postal code. A 3rd-order identifier might be a visual item, like a rainbow flag, being tied

back to either sexual orientation or gender. This concept of re-identification is also important at a technical level as well. For example, the NY State Senate Bill 8448--C includes a provision making it unlawful for "covered entities" to "attempt to re-identity" individuals.

Entities providing digital contract tracing apps or services should include provisions in contract with any other entities prohibiting intentional or unintentional re-identification of users. For example, see the Model DPA for Government for the Development of Exposure Alerting Applications and Systems contract clause:

"De-identified Data" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer and that has been protected by (i) technical safeguards that prohibit reidentification of a natural person; (ii) business processes that specifically prohibit reidentification of the information; (iii) business processes that prevent inadvertent release of de-identified information. The method of creating Deidentified Data shall be made publicly available and shall comply with data de-identification best practices, for example the HIPAA standard."[26]

De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information while protecting privacy. Several U.S. laws, regulations and policies specify that data should be de-identified prior to sharing. In recent years researchers have shown that some de-identified data can sometimes be re-identified.

In the future, we foresee and recommend embracing emerging cryptographic measures to protect identity (hashtree of identity attributes, homomorphic encryption, algorithmic protections like OPAL,[27] etc.) when they become more widely available.

Transparency

> *Users should be given notice of an organization's information gathering, retention, uses, practices, and privacy policies before any personal information is collected from them. Organizations should explicitly state the following:*
>
> - *identification of the entity collecting the data;*
> - *identification of the uses to which the data will be put;*
> - *identification of any potential third-party 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; and,*

> - *whether the data is being collected in compliance with a jurisdiction's laws regarding privacy and intended use.*
>
> *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.*

While contact tracing is regarded as a valuable tool of public health, it can only achieve that function through the acceptance and efforts of the individual acting in a collective. For many, participating in contact tracing highlights a conflict between societal good and individual rights and security and thus operators of contact tracing must foster a welcoming and trustworthy environment for the individual. Transparency honors the individual with knowledge, clarity, and assurance about the requirements and potential risk associated. Transparency offers the individual an implicit choice to make an informed choice, which, in turn, empowers them to consciously and willingly support the collective good. Transparency is foundational to building trust and building trust is foundational to digital contact tracing.

Accountability

> *In order to ensure that organizations adhere to contact tracing privacy principles, there must be enforcement measures, such as: self-regulatory efforts undertaken by those collecting information for digital contact tracing apps or some 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.*

In a broad sense, accountability refers to the inclusion of all relevant stakeholders within the existing digital contact tracing ecosystems. At a basic level, these connections help build understanding about the specific needs of each party within the network and help arrive at informed solutions that accurately reflect a balance of interests across these communities. Accountability does not stop with the inclusion of all of the interested parties mentioned in the principle.

Absent any mechanisms to hold wrongdoers accountable for their actions, there remain strong incentives for businesses and governments to use the data outside the scope of its intended use. To that end, it is important for these ecosystems to develop a comprehensive set of mechanisms that

serve as incentives to be accountable to the rest of the community. Some of these mechanisms can include proactive self-regulation by those parties involved with developing contact tracing apps, designing terms of service and terms of use in such a way that provides users of digital contact tracing apps with clear paths to file a cause of action, and clear rules for when government enforcement is necessary in either a civil or criminal context.

In order to ensure accountability measures are suited to the needs of a particular community, it remains important to listen to the concerns of all involved, develop proactive and reactive strategies for holding each other accountable, and continually updating these strategies in light of new developments.

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.*

Proportionality refers to the balance between the projected/estimated benefit of a solution when weighed against potential risks. In an efficacy and usefulness context, proportionality in digital contract tracing can be achieved in part with disease burden data, which is defined as the impact of a health problem as measured by financial cost, mortality, morbidity, or other indicators.[28] n a privacy context, the term considers the quantifiable/measurable benefit of a contact tracing solution compared to the risk of invasion of privacy created by the program. At this point in the current pandemic, because of the fluid nature of the tools/programs in development, proportionality must be continually evaluated and considered against an assessment period which can allow for an ongoing balancing test to determine proportionality on a rolling basis.

Relevant factors to consider in such an ongoing evaluation should include:

- On the efficacy and usefulness side of the equation: reducing the burden of disease such as by enabling earlier detection and prevention, decreasing *the incidence of new cases, hospitalizations, morbidity and mortality and measurably augmenting manual contact tracing methods; and*
- On the privacy side of the equation*: reported actual privacy violations, assessment of the* scope and purpose of the contact tracing app, the type(s) of data collected, collection processes, sharing, retention, and deletion of data.

In EU law, four stages are described as related to a proportionality test:

- there must be a legitimate aim for a measure;
- the measure must be suitable to achieve the aim (potentially with a requirement of evidence to show it will have that effect);
- the measure must be necessary to achieve the aim, that there cannot be any less onerous way of doing it; and,
- the measure must be reasonable, considering the competing interests of different groups at hand.[29]

The concept of proportionality is not an uncommon legal and policy criterion. For example, proportionality is also used as a legal test of fairness and justice, interpretation of statutes, processes, and as a method that aids in discerning balance between restriction and corrective measures. Some contact tracing (mobile) apps are no more than anonymous surveys, that are voluntary and ask for checks of apparent and visible symptoms associated with COVID-19. Apps that do not require personal information would have only the requisite amount of potentially linkable network attributes that are associated with the mobile device, the network provider (ISP) and the collector (a public health agency) and while these would present a low risk to privacy they may also be less efficacious.

Inasmuch that there is no requirement to provide PHI (Personal Health Information) or personal information, and that in all likelihood device identifiers are not transmitted to the collector, there would not be a *de facto* or *de jure* acquisition of personal information in violation of privacy or health data protection legislation. This however does not guarantee that, given resources, passive collection may not occur.

In the case of a pandemic, the rapid spread of a highly contagious virus is the greater danger if mitigation measures are not applied. At the same time, intermediaries, such as ISPs, public health agencies, and health providers must abide by and actively uphold cybersecurity practices as prescribed by law (GDPR, HIPAA, Privacy Act, etc.).

3. Other Pillars

In addition to the privacy principles, we have also identified these other pillars that are not so much related to privacy as they are to the broader ecosystem of digital contact tracing apps. Here, we provide insight about why we believe these principles are important and how they directly connect with the principles stated above.

Voluntary

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

Voluntariness was originally included in our list of privacy principles. However, we removed it because of the global scope of these principles and the acknowledgement that circumstances may arise where digital contact tracing should and ought to be compulsory. In this regard, voluntariness in these principles can be understood as occupying some area between lawfulness, informed consent, and proportionality. In all cases where it is proportional to the threat requiring contact tracing, the use of digital contact tracing apps should be voluntary.

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.*

Originally, this had been included under right to control. However, we removed it from that principle because the thrust of what this pillar is addressing is broader and adjacent to the actual ability to control the way that data is used in digital contact tracing applications. We do also see connections between this pillar and other principles as well. Understanding potential downstream uses of data, such as data aggregation, is relevant to providing informed consent and also to transparency. New uses of aggregated data further underscore the need to continually provide fresh consent to purported uses. In all cases when a third party is aggregating data, it is important to specify exactly why the data is being used, who has access to this data, and what precautions are in place to reduce re-identification of the data.

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.*

Security is a pillar that is included in some of the other principles that we had surveyed. We see security as being a technical matter for preserving the integrity of digital contact tracing apps, and therefore believe it has a place in the digital contact tracing ecosystem. However, we believe that because the mechanics of security are conceptually different from the mechanics of privacy it ought to be listed as a pillar. One of the most important characteristics about security is that it is a fluid and continually changing state. What is secure today may not be secure tomorrow. For this reason, it is important for those conducting digital contact tracing to properly log the efforts undertaken to secure the digital contact tracing system, analyze these efforts in light of advances in technology and information security, and update them accordingly.

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.*

The thinking around the pillar of Effectiveness informed much of the thinking around Proportionality and vice versa. Digital contact tracing apps should be designed in a way that is effective at achieving a stated goal. In many cases, these goals will relate to epidemiology and, as such, should be tethered to measurable and auditable epidemiological standards to ensure that such applications will provide a benefit to those who are using them.

Usability

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

Digital contact tracing apps will only be effective at achieving their purpose to the extent that they are usable. By endeavoring to design digital contact tracing apps in accordance with widely recognized and adopted standards, such as those of the World Wide Web Consortium and the W3C Web Accessibility Initiative, that make the web usable and accessible, these apps will have fewer liabilities and ultimately prove to be more trustworthy.

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.*

It is important to acknowledge that digital contact tracing apps only work if a person has a mobile device. For a large percentage of the world, this is not the case. Further, the effects of pandemics frequently impact communities disproportionately. Being mindful of these disparate impacts and working to develop strategies that take into account these unique considerations is something that should be present throughout the conversations that lead to the creation of digital contact tracing apps.

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.

Footnotes

1. Most notably, our work was referenced in *Digital Contact Tracing for Pandemic Response*, a book published by John Hopkins University. *See* Kahn, Jeffrey and John Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies, *Digital Contact Tracing for Pandemic Response*. John Hopkins University Press, 2020. Project MUSE. doi:10.1353/book.75831. Available at: https://muse.jhu.edu/book/75831/pdf. ↩
2. Many of the definitions included in this list borrow from ForHumanity's "Independent Contact Tracing Audit." Available at: https://www.forhumanity.center/contact-tracing-audit. ↩
3. Huang, Y., Tang, J., Tam, W. W., Mao, C., Yuan, J., Di, M., & Yang, Z. (2016). Comparing the Overall Result and Interaction in Aggregate Data Meta-Analysis and Individual Patient Data Meta-Analysis. *Medicine*, *95*(14), e3312. https://doi.org/10.1097/MD.0000000000003312. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4998822/ ↩
4. General Data Protection Regulation (GDPR) Article 7. Available at: https://gdpr.eu/article-7-how-to-get-consent-to-collect-personal-data/ (last visited August 8, 2020). ↩
5. *See e.g,* Simson Garfinkel, "NISTIR 8053" National Institute of Standards and Technology, 2015. Available at: https://csrc.nist.gov/publications/detail/nistir/8053/final. ↩
6. Our definition borrows from the United States Centers for Disease Control and Prevention definition of Exposure Notification from "Notification of Exposure: A Contact Tracer's Guide for COVID-19" and generalizes for application to broader and additional contexts of Contact Tracing. Available at: https://www.cdc.gov/coronavirus/2019-ncov/php/notification-of-exposure.html (last visited August 8, 2020). ↩
7. *Id.* ↩
8. Model State Emergency Health Powers Act (MSEHPA). Art. 1. Sec. 104(m). https://www.aapsonline.org/legis/msehpa.pdf. ↩
9. General Data Protection Regulation (GDPR) Article 9. Available at: https://gdpr-info.eu/art-9-gdpr/ (last visited August 8, 2020). ↩
10. U.S. Const. amend IV. ↩
11. *Smith v. Maryland*, 425 U.S. 435 (1979) "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will

be used only for a limited purpose and the confidence placed in the third party will not be betrayed"; *Id.* at 446 signaling *U.S. v. White*, 401 U.S. 745, 751-752 (1971). ↩

12. *United States v. Miller*, 425 U.S. 435 (1976). ↩

13. *United States v. Forrester*, 512 F.3d 500, 509-510 (9th Cir. 2007). "Like telephone numbers, which provide instructions to the 'switching equipment that processed those numbers," e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.'" *Id.* at 509 citing *Smith v. Maryland,* 425 U.S. 735, 744 (1979). ↩

14. Contact Tracing Bill of Rights. Available at: https://github.com/TCNCoalition/TCN/blob/main/ContactTracingBillOfRights.md. ↩

15. Yves-Alexandre de Montjoye, Florimond Houssiau, Andrea Gadotti, Florent Guepin, "Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask." Computational Privacy Group. April 2, 2020. Available at: https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/. ↩

16. "10 requirements for the evaluation of 'Contact Tracing' apps" Chaos Computer Club. April 6, 2020. Available at: https://www.ccc.de/en/updates/2020/contact-tracing-requirements. ↩

17. Cari Spivack, Andrew Trask, Harper Reed, "Data Rights for Exposure Notification" Available at: https://exposurenotification.org/. ↩

18. "Coronavirus: Guidance to ensure full data protection standards of apps fighting the pandemic" European Commission. April 16, 2020. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_669. ↩

19. Andrew Crocker, Kurt Opsahl, Bennett Cyphers, "The Challenge of Proximity Apps For COVID-19 Contact Tracing" Electronic Frontier Foundation, April 10, 2020. Available at: https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing. ↩

20. Jay Stanley, Jennifer Stisa Granick. "The Limits of Location Tracking in an Epidemic" the American Civil Liberties Union, April 8, 2020. Available at: https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic. ↩

21. Ashkan Soltani, Ryan Calo, Carl Bergstrom, "Contact-tracing apps are not a solution to the COVID-19 crisis" The Brookings Institution, April 27, 2020. Available at:

https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/. ↩

22. Jonathan Zittrain, Urs Gasser, Mary Gray, Kade Crockford, "Digital Contact Tracing: Perspectives on approaches to COVID-19" Berkman Klein Center for Internet & Society at Harvard University, June 25, 2020. Available at: https://cyber.harvard.edu/story/2020-06/digital-contact-tracing-perspectives-approaches-covid-19. ↩

23.

1. Kahn, Jeffrey and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies. Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance. Johns Hopkins University Press, 2020. Project MUSE. doi:10.1353/book.75831. Available at: https://muse.jhu.edu/book/75831/pdf.

↩

24. General Data Protection Regulation (GDPR) Article 6. Available at: https://gdpr.eu/article-6-how-to-process-personal-data-legally/ (last visited August 8, 2020). ↩

25. *See* General Data Protection Regulation (GDPR). Available at: https://gdpr.eu/ (last visited August 8, 2020).*See also*, The Federal Trade Commission (FTC), *Fair Information Practice Principles*, 2010. Available at: https://web.archive.org/web/20090311134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm. ↩

26. Cari Spivack, Coleen Brown, Dean Forbes, Michael R. Roberts, "Model DPA for Government for the Development of Exposure Alerting Applications and Systems." MIT Computational Law Report, May 20, 2020. Available at: https://law.mit.edu/pub/modeldpaforgovernment. ↩

27. Thomas Hardjono, Alex "Sandy" Pentland, "Open Algorithms for Identity Federation" arXiv:1705.10880v2 [cs.CY] 24 Oct 2017. Available at: https://arxiv.org/pdf/1705.10880.pdf. ↩

28. "Metrics: Disability-Adjusted Life Year (DALY)" World Health Organization. Available at: https://www.who.int/healthinfo/global_burden_disease/metrics_daly/en/. ↩

29. Paul Craig and Grainne de Burca, *EU Law* (5th edn OUP 2011) p. 526. ↩