INTERNATIONAL COMPUTATIONAL LAW JOURNAL

CODEX SOURCE ARCHIVE

COVID-19 Contact Tracing Privacy Principles – Audit Framework

ForHumanity

Computational Law Report · Special Release: COVID-19 · 2020-11-20

Reader edition prepared by The Research University under CC BY 4.0. This cover was added; the original PDF pages follow unchanged. Original authorship, publication identity and source links are preserved. This independent republication is not sponsored or endorsed by Stanford University, Stanford Law School, CodeX or MIT.

Volume 1 · Issue 3 · Emergency Technology, Privacy and Public Trust

Original source and license evidence are recorded on the article landing page.

MIT Computational Law Report

COVID-19 Contact Tracing Privacy Principles - Audit Framework

ForHumanity

Published on: Nov 20, 2020

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

In response to the overwhelming need for trust enhancements to Contact Tracing solutions around the world, this report on Contact Tracing Privacy Principles is publishing the Independent Audit and Governance of Contact Tracing, developed by ForHumanity[1] and made available under Creative Commons Non-Commercial, Non-Derivative license. Our intent by sharing this audit and assessment criteria is to demonstrate that transparency, disclosure and third-party oversight can be valuable pathways to enhancing trust in digital contact tracing solutions.

Independent Board of Governance

Following a series of corporate and accounting scandals in the late 90s and early 00s, the US Congress passed the Sarbanes-Oxley Act of 2002 (SOX).[2] The act, in Title II, codified the term "Independence," with nine sections of standards defining external auditor independence designed to minimize conflicts of interest. The practical application of SOX is to ensure that independent auditors have no or limited ability to gain from asserting corporate compliance with accounting standards, where they are non-compliant. Establishing the relationship between external auditors and corporations where the audit has liability for asserting compliance when there is a failure. This relationship of independence is the hallmark of trust in a worldwide system that widely uses audited financial statements with the embedded assumption of trustworthiness.

The independent board of governance exists to provide transparency, oversight and a lens of global best-practices on the contact tracing authority's program for the duration of its operation. The board would be populated with experts who are steeped in the ForHumanity digital contact tracing audit and are regularly examining best practices around the world. They exist to execute the mantra "trust but verify" and to collaborate with the contract tracing authority to enhance trust between the traced public and the digital contract training solution enabling it to be a valuable tool of public health.

Independent Audit

The Independent Audit is the tool of discovery and verification of compliance built on the model of financial auditing. Many jurisdictions require independent financial audits[3]. This form of third-party oversight, with a transparent set of well-established, consensus-driven rules, has created a level of trust with financial accounts. This level of trust is especially important for contact tracing. This report asserts that these same principles will dramatically enhance the infrastructure of trust for contract tracing systems. Trust and bridging the "trust-gap" between contact tracing authorities and the traced remains a key ingredient missing for voluntary digital contact tracing systems to be effective.

Independent Audit of AI Systems (IAAIS) Classifications

Built on the same foundation as Independent Audit of AI Systems (IAAIS), the audit examines the contact tracing program from five (5) key perspectives, knowns as IAAIS classifications:

1. Ethics
2. Privacy
3. Trust
4. Bias
5. Cybersecurity

Then uniquely for contact tracing it also examines three (3) additional factors:

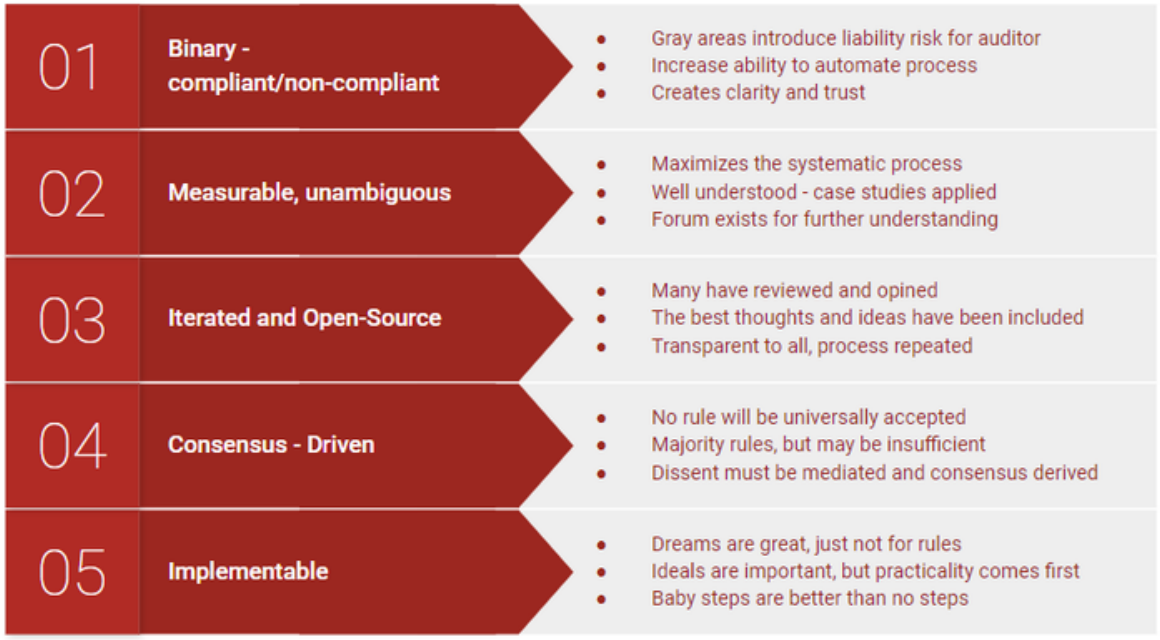
1. Launch
2. Features and execution of the technology
3. Expiry

This comprehensive approach to contact tracing will provide an independent board of governance the tools and information it requires to fairly and responsibly oversee the contact tracing program.

The audit is a combination of information gathering and best practices suggestions. The level of compliance will vary across programs. Many will be unable to meet the highest standard of compliance, while others will find their systems are mostly compliant but need some tweaking to satisfy the audit. Certain characteristics of some contact tracing programs render them virtually unauditable, such as mandatory participation. ForHumanity offers to work with the contact tracing authority for remediation as the mission of this endeavor is to increase the trust in contact tracing systems, not be a watchdog or outright critic.

Audit Questions

The approach focuses each question on achieving these characteristics:



These questions are compiled to achieve complete understanding and assurance around every aspect of the contact tracing program, especially the technology.

Audit Documentation

There are no ambiguous answers in the audit. Documentation, testing, legislation, pictures, and graphics are required pieces of audit documentation. Each question has a predetermined set of criteria expected by the auditors to satisfy the audit. Some testing will be outsourced, such as third-party testing which will validate that the technical features and technical specification of the technology conform to the audit rules.

Best Practices

The team of ForHumanity Fellows has also identified some aspects of the audit which denote best practices. In some cases, having a certain feature of your contact tracing system (e.g. being mandatory) also constitutes something distinctly below best practices. Finally, there are some questions that simply reflect the preferences or legal requirements of the contact tracing authority.

An example of this is *Q9 Does your contact tracing program use human contact tracers*?

The Fellows reviewing the audit felt that there were pros and cons to a "yes" to this answer. It seems clear that some contact tracing programs which do not use humans are likely to be more privacy-protecting, but may be considered less personal and compassionate. Making a choice here is, in some cases, a matter of preference of one value system over another.

Definitions

Similar to a contract with predefined terms, the audit uses bold and capitalized terms to denote predefined terminology. An important one, repeated many times is **Contact Tracing Entity (CTE)** which is defined *as a person or organization having power or control to conduct a contact tracing program.*

Commentary

Everyone is welcome to leave comments in the audit. Some of these edits will be resolved and disappear, others have been left there so that readers may understand the nuance and backstory for some of the audit questions. This is a living document and ForHumanity encourages scrutiny, questions, suggestions, and debate. Comments may be offered directly in the Google Sheets document.

Updates to the Audit

On a regular basis, the ForHumanity Fellows for contact tracing will review proposed changes, added questions, and update the latest version of the audit. As of publication today we are on version 2.5. Supermajority of the ForHumanity Fellows is the requirement for a new rule to be added, definition to be changed or word choice to be altered.

Viewing the Audit

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

The Audit is open and transparent to all who would like to examine it. ForHumanity asks you to register on the website, linked here: https://www.forhumanity.center/registration-1. Once registered, one is invited to examine and comment on the audit in Google Sheets. A snapshot version 2.5 of the audit is also available as part of this MIT Computational Law Report Special Release on COVID-19, here: *https://docs.google.com/spreadsheets/d/e/2PACX-1vSGm82lg6nhr15IK8RFNnjIjA5-cKCjoou3cdF9DOUD44dONkSD4_1wzDoktu-Qin2J8nQKuousjcTZ/pubhtml?gid=0&single=true*

Footnotes

1. "Contact Tracing Governance — ForHumanity." https://www.forhumanity.center/contact-tracing-governance-1. Accessed 28 Aug. 2020. ↩

2. "H.R.3763 - 107th Congress (2001-2002): Sarbanes-Oxley Act ...." https://www.congress.gov/bill/107th-congress/house-bill/3763. Accessed 28 Aug. 2020. ↩

3. "Use of IFRS Standards by jurisdiction - IFRS.org." https://www.ifrs.org/use-around-the-world/use-of-ifrs-standards-by-jurisdiction/. Accessed 28 Aug. 2020. ↩