

Undergraduate Thesis Prospectus

Mobile Contact Tracing Software
(technical research project in Computer Science)

**Contact Tracing and Privacy
amid the COVID-19 Pandemic**
(sociotechnical research project)

by

Sean Burtner

November 2, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Sean Burtner

Technical advisor: Aaron Bloomfield, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

General research problem

How has software been used to alleviate public health burdens?

Software has become an invaluable tool in the battle against disease. Countless programs, statistical packages, and models have been developed to collect and process health-related information faster. For example, over 95 percent of hospitals in the U.S. have adopted an electronic health record system (Parasrampur & Henry, 2019). The health care sector is consequently better equipped for “surveillance, disease control interventions, and delivery of clinical services” (McCullough & Goodin, 2016). Yet such intensive and extensive medical surveillance inevitably raises problems of privacy and public distrust, which, if poorly managed, may induce public resistance that curtails the advantages such systems have to offer.

Mobile contact tracing software

How effective are mobile contact tracing apps?

The technical project will be completed in the spring semester. Consequently, the exact scope of the project is not currently defined, though it will likely entail a literature review analyzing the security and efficacy of contact tracing software; this will be formally established early in the spring semester. The capstone project will be conducted individually under the supervision of Aaron Bloomfield in the computer science department.

Historically, health authorities conducted contact tracing by manually interviewing infected patients to identify other individuals at risk of infection. The ubiquity of mobile phones has created an opportunity to digitize this task. Contact tracing software can be designed in various ways, and each unique design presents its own set of security vulnerabilities and privacy issues (Ahmed et al., 2020). The ways in which data are stored, exchanged, and processed dictate the type of vulnerabilities in each design. However, regardless of the specific architecture, strong

security and privacy measures are critical in obtaining the public's trust, and a high adoption rate in the end. The success of any contact tracing app is highly contingent on a sufficient adoption rate of at least 60% (Altmann et al., 2020). It is therefore imperative to retain public confidence by designing secure, effective software.

This project seeks to understand the advantages and disadvantages of various contact tracing app architectures with regard to their security, privacy, and overall efficacy. This analysis will then be applied to the Virginia Department of Health's (VDH) contact tracing app called COVIDWISE. Several studies of this nature exist which analyze other contact tracing apps from around the world. This project will extend the current body of work to include COVIDWISE. Technical specifications of the app, as well as the source code, are available via the VDH website. These resources will enable the high-level analysis of contact tracing app designs to be concretely applied to the COVIDWISE app; the final product will be a paper containing both the general investigation of different app designs and the COVIDWISE analysis. Verifying the app's security and efficacy is an important step in achieving a high adoption rate, and therefore in combatting the spread of the virus.

Contact tracing and privacy amid the COVID-19 pandemic

In the U.S., in response to the 2020 pandemic, how have public health authorities, privacy advocates, and other social groups competed to draw the line between essential contact tracing and undue invasion of privacy?

Contact tracing has been essential to efforts to slow the spread of epidemic disease, including COVID-19. Tracers identify recent contacts of infected persons so that preventive measures may be taken. Even manual contact tracing can raise problems of privacy, but mobile contact tracing apps now partly automate the process. Some critics contend that such techniques

can constitute invasions of privacy. To work, contact tracing must be trusted. According to Ferretti et al. (2020), the speed and efficiency of contact tracing apps could “achieve epidemic control if used by enough people.”

Researchers have examined common misgivings about contact tracing techniques, and have proposed ways to address them. Ahmed et al. (2020) contend that “complete transparency and legislative guarantees against misuse of data” are essential to obtaining the public’s trust. Altmann et al. (2020) similarly found that trust in government is an “important determinant of support” for this technology, justifying transparent, yet stringent, security measures. They also found much less trust of the software in the U.S. than in other countries, which likely reflects low trust in government. These findings are complemented by those of Keusch et al. (2019), who concluded that the primary reservations about mobile data collection are related to privacy and data security. The researchers also found that people who have a contact tracing app have little incentive to use it, and insufficient information about data usage to trust it.

The American Civil Liberties Union warns of “significant risks to privacy, civil rights, and civil liberties” from contact tracing technology (Gillmor, 2020). It has issued technology principles intended to guide the developers of contact tracing applications. Apple and Google publicly announced a joint effort to develop contact tracing functionality in iOS and Android devices, and are alert to the skepticism; Apple has assured the public that “user privacy and security [are] central to the design” (Apple, 2020). Public health agencies, such as the Virginia Department of Health (VDH), strive to retain public trust while preserving the public good. To promote adoption of the COVIDWISE app, the VDH (2020) published an explanation of how it works, similarly emphasizing its “privacy-preserving” anonymity. The U.S. Centers for Disease Control and Prevention (CDC) sponsors research, publishes data, and issues recommendations to

limit the spread of disease in the United States. The CDC has issued guidelines to the states to preserve “personal privacy and data security” in their contact tracing techniques (CDC, 2020).

The Electronic Privacy Information Center (EPIC) is an advocacy that promotes strict privacy safeguards on contact tracing technology to protect “individual freedoms and rights” (Rotenberg et al., 2020). In April 2020, EPIC urged Congress to regulate digital contact tracing, especially the collection of personally identifiable information. The Electronic Frontier Foundation (EFF), another advocacy, maintains that any contact tracing app “needs rigorous security testing and data minimization” (EFF, 2020). EFF is a strong privacy advocate; it opposes any contact tracing based on phone location data, and further claims that “any use of aggregate location data to inform public health decisions” requires safeguards. Public Knowledge, a digital policy advocacy, also calls for strong privacy protections. It commended several U.S. senators for introducing the Public Health Emergency Privacy Act that would serve to “provide meaningful privacy, security, and civil rights protections for Americans’ data” collected by contact tracing technology (Stella, 2020). These social groups compete to influence the extent and nature of digital contact tracing, thereby influencing its adoption rate and its efficacy.

References

- Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Seneviratne, A., Hu, W., Janicke, H., & Jha, S. K. (2020). A survey of COVID-19 contact tracing apps. *IEEE Access*, 8, 134577-134601. <http://doi.org/10.1109/access.2020.3010226>
- Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., & Abeler, J. (2020). Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth and uHealth*, 8(8), e19857. <https://doi.org/10.2196/19857>
- Apple. (2020, April 10). Apple and Google partner on COVID-19 contact tracing technology. Apple Newsroom. <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>
- CDC (2020). U.S. Centers for Disease Control and Prevention. Guidelines for the implementation and use of digital tools to augment traditional contact tracing. Centers for Disease Control and Prevention. <https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/guidelines-digital-tools-contact-tracing.pdf>
- EFF (2020). Electronic Frontier Foundation. COVID-19 and digital rights. Electronic Frontier Foundation. <https://www.eff.org/issues/covid-19>
- Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., & Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, 368(6491). <http://doi.org/10.1126/science.abb6936>
- Gillmor, D. K. (2020, April 16). Principles for technology-assisted contact-tracing. American Civil Liberties Union. <https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing>
- Keusch, F., Struminskaya, B., Antoun, C., Couper, M. P., & Kreuter, F. (2019). Willingness to participate in passive mobile data collection. *Public Opinion Quarterly*, 83(1), 210-235. <https://doi.org/10.1093/poq/nfz007>
- McCullough, J. M., & Goodin, K. (2016). Clinical data systems to support public health practice: A national survey of software and storage systems among local health departments. *Journal of Public Health Management and Practice*, 22(6), S18–S26. <https://doi.org/10.1097/PHH.0000000000000443>
- Parasrampur, S. & Henry, J. (2019). Hospitals' use of electronic health records data, 2015-2017. The Office of the National Coordinator for Health Information Technology. <https://www.healthit.gov/sites/default/files/page/2019-04/AHAEHRUseDataBrief.pdf>

Rotenberg, M., Fitzgerald, C., & Butler, A. (2020, April 15). EPIC to Congress: Establish privacy safeguards for digital contact tracing. Electronic Privacy Information Center. <https://epic.org/2020/04/epic-to-congress-establish-pri.html>

Stella, S. (2020, May 14). Public Knowledge welcomes privacy bill protecting American data during pandemic. Public Knowledge. <https://www.publicknowledge.org/press-release/public-knowledge-welcomes-privacy-bill-protecting-american-data-during-pandemic/>

Virginia Department of Health. (2020). COVIDWISE. Virginia Department of Health. <https://www.vdh.virginia.gov/covidwise/>